الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne démocratique et populaire

وزارة التعليم العالي و البحث العلمي
Ministère de l'enseignement supérieur et de la recherche scientifique

جامعة سعد دحلب البليدة
Université SAAD DAHLAB de BLIDA

كلية التكنولوجيا
Faculté de Technologie

قسم الإلكترونيك
Département d'Électronique

Mémoire de Master

Mention Électronique
Spécialité Réseaux et Télécommunications

présenté par

ALLAL Nadjib

&

EL BLIDI Othmene

Détection de l'utilisation du Réseau Tor dans une entreprise.

Proposé par : Dr.MEHDI Merouane

Année Universitaire 2017-2018

Remerciements

Avant tout, nous remercions le Dieu tout puissant de nous avoir permis de marcher sur le chemin de la science, et aujourd'hui d'effectuer ce travail. À mes parents pour leur soutenu et pour tous les sacrifices consentis, ainsi qu'à tous mes frères et sœurs

Nous remercions notre enseignant et directeur du mémoire Mr. MEHDI M. d'avoir accepté notre encadrement, et de nous avoir assistés durant cette période, en nous accordant toute l'attention et le temps qu'il faut.

Nous tenons à remercier messieurs les membres du jury d'avoir accepté d'évaluer notre travail.

Nos remerciements s'adressent également à l'équipe pédagogique de département d'électronique d'Université Saad Dahlab Blida 1 d'avoir assurée la partie théorique de notre formation.

Enfin, à tous ceux qui de près ou de loin ont contribué moralement ou matériellement à l'aboutissement de ce travail.

Nous disons merci.

Dédicace

Je dédie ce travail à mes chers parents qui se sont sacrifiés pour ma réussite,

Mon père, celui qui a inséré le sens de la responsabilité en moi, qui m'a toujours soutenu moralement et financièrement.

A ma très chère Maman, celle qui n'a jamais cessé de me soutenir, grâce à elle je ne baisserai jamais les bras,

A mes chers frères et sœur.

A tous mes amis qui ont toujours été là pour moi à savoir ceux qui sont avec moi en Algérie et ceux qui sont ailleurs. je vous remercie du fond du cœur.

ملخص:

استعمال " الشبكة طور" في شبكة الشركات غير منصوح به، لأنه بإمكانها أن تعرض الشركة لعدة مخاطر امنية ومشاكل قضائية.

الهدف من هذه الإشكالية المطروحة هو الكشف عن استعمال " الشبكة طور" والذي يتطلب تحليلا لتدفق البيانات الويب " الشبكة طور" وكذلك الويب العادي واجراء مقارنة بينهما. من خلال اختلاف بين التدفقين تستخرج بصمة رقمية تسمح بالتعرف على "الشبكة طور". تطبيق هذه البصمات الرقمية في نظام كشف الاختراقات الشبكة "سنورة" يسمح باكتشاف استعمال "الشبكة طور".

كلمات المفاتيح: الشبكة طور، تحليل التدفق الويب، البصمات الرقمية، سنورة ، نظام كشف الاختراقات الشبكة.

Résumé :

L'utilisation du réseau Tor dans les entreprises n'est pas conseillée, car peut exposer l'entreprise à divers risques de sécurité et à des problèmes judiciaires.

L'objectif de cette thèse est la détection de l'utilisation de réseau Tor. La détection de ce dernier nécessite une analyse du trafic web du réseau Tor et celle du web normal et faire une comparaison entre les deux. Les différences entre les deux trafics et le relèvement des empreintes digitales permettent d'identifier le réseau Tor. L'implémentation du ces empreintes dans le système de détection d'intrusion réseau (NIDS) Snort permet la détection de l'utilisation du réseau Tor.

Mots clés : Réseau Tor ; Analyse du trafic web; Empreintes digitales ; NIDS ;Snort.

Abstract :

The use of the Tor network in companies is not advisable because it can expose the company to various security risks and judicial problems.

The goal of this thesis is the detection of Tor network usage. The detection of the use of the Tor Network, which requires an analysis of the web traffic of the Tor network and that of the normal web and make a comparison between the two. The differences between the two traffics and the fingerprinting make it possible to identify the Tor network. The implementation of these fingerprints in Network Intrusion Detection System (NIDS) Snort allows the detection of Tor network usage.

Keywords: Tor network; Analysis of web traffic; digitals prints; NIDS; Snort.

Listes des acronymes et abréviations

API	Application Programming Interface.
AES	Advanced Encryption Standard.
ACK	Acknowledgment.
BASE	Basic Analysis and Security Engine.
DHCP	Dynamic Host Configuration Protocol.
DNS	Domain Name Service.
FAI	Fournisseur d'Accès à Internet.
FDDI	Fiber Distributed Data Interface.
FFDHE	Finite Field Diffie-Hellman Ephemeral Parameter.
FTP	File Transfer Protocol.
HTML	Hyper Text Markup Language
HIDS	Host Based Intrusions Detection System.
HTTP	HyperText Transfer Protocol.
HTTPS	HyperText Transfer Protocol Secure.
ICMP	Internet Control Message Protocol.
IDS	Intrusions Detection System.
IEEE	Institute of Electrical and Electronics Engineers.
IETF	Internet Engineering Task Force.
IP	Internet Protocol.
IPS	Intrusions Prevention System.
IPSec	Internet Protocol Security.
IPv4	Internet Protocol version 4.
L2TP	Layer 2 Tunneling Protocol.
MAN	Metropolitan Area Network.
MAC	Media Access Control (niveau 2 LAN).
NAT	Network Address Translation.
NIDS	Network Based Intrusions Detection System.
NSA	National Security Agency.
OSI	Open Systems Interconnection.
POP3	Post Office Protocol Version 3.
PPP	Point to Point Protocol.
PPTP	Point-to-point tunneling protocol.
RSA	Au nom de Ronald Rivest, Adi Shamir et Leonard Adleman
SMTP	Simple Mail Protocol Protocol.
SSL	Secure Socket Layer.
SYN	Synchronize.
TCP	Transmission Control Protocol.
TLS	Transport Layer SecurityUDP User Datagram Protocol.
TOR	The Onion Router.
URL	Uniform Resource Locator.
VPN	Virtual Private Network.
WAN	Wide Area Network.

Table des matières :

Liste des figures

Liste des tableaux

Introduction générale

Aujourd'hui, presque tout ce qu'on fait sur Internet laisse une empreinte numérique qui décrit nos activités et précise leurs emplacements. Désormais, nous devons être prudents car cet océan d'empreintes nous décrit, d'une manière complète et avec un réalisme effrayant, d'où survient la question de l'anonymat et la protection de la vie privée en ligne.

Pour minimiser nos empreintes sur Internet, il existe plusieurs systèmes qui permettent de conserver un certain anonymat, comme Proxy, VPN et réseau Tor. Le réseau Tor est depuis quelques années, sans doute le plus connu des technologies permettant l'anonymat sur Internet. Le réseau Tor, grâce à sa technique de routage en oignon, permet d'anonymiser les connexions sur internet.

Le réseau Tor et comme tout système possède un côté sombre. Celui-ci est souvent utilisé par des individus mal intentionnés dans des activités malveillants ou criminelles ou d'autres types d'actes répréhensibles.

L'utilisation de cet outil dans d'un réseau d'entreprise peut exposer l'entreprise à divers risques de sécurité et à des problèmes judiciaires. En effet, les organisations et entreprises doivent commence, depuis quelques temps à prêter attention au risque, lors l'utilisation du réseau Tor dans leur réseau.

Cependant, la détection de réseau Tor dans un réseau d'entreprise est très compliquée car nécessite des techniques d'analyse des données et des mises à jour permanentes des règles de sécurité (adresses IP, empreintes, etc.). Les organisations et entreprises devraient envisager le déploiement de plusieurs solutions. Afin augmenter les chances d'empêcher l'utilisation de système dans leur réseau d'entreprise.

Les systèmes de détection d'intrusion réseau (NIDS) permettent la détection de l'utilisation de réseau Tor, par l'analyse de flux de données en temps réel par rapport à une base de données de signatures.

- **Problématique :**

Au vu de tout ce qui précède, la question principale, à laquelle nous tenterons de répondre à travers cette étude, est la suivante :

La détection de l'utilisation du navigateur Tor dans une entreprise, va-t-elle être possible ?

De cette problématique découlent les questions secondaires suivantes :

- Qu'est-ce que le réseau Tor et quels sont ses éléments ?
- Y a-t-il une signature qui peut différencier le trafic Tor sur le trafic web normal?
- Peut-on implémenter ces signatures dans un système de détection d'intrusion réseau ?

- **Méthodologie de recherche :**

Dans le cadre de préparation de notre mémoire de fin d'étude, qui porte essentiellement sur la détection de l'utilisation de navigateur Tor dans une entreprise, on a suivi une méthodologie de recherche théorique et pratique.

Théorique, basée sur la recherche documentaire auprès des bibliothèques virtuelles de recherche qui nous ont permis de consulter plusieurs ouvrages numériques afin de définir les concepts théoriques sur le sujet de notre recherche.

Pratique, basée sur l'analyse du trafic web provenant du réseau Tor et celle du web normal suivi par l'implémentation d'un système de détection d'intrusion réseau Snort. Pour alors nous avons validé notre travail par des tests réels avec simulation.

- **Structure du mémoire :**

Pour présenter notre travail, nous avons scindé notre mémoire en quatre chapitres. Dans le premier chapitre, on présente les concepts de base des réseaux informatiques. Le second chapitre, traite l'anonymat et ses outils et plus particulièrement le réseau Tor et son infrastructure. Le troisième chapitre concerne l'analyse du trafic web provenant du réseau Tor et celle du web normal et le relèvement d'une empreinte digitale permettent d'identifier le réseau Tor. Le dernier chapitre sera consacré à la mise en œuvre de Snort. Et au test de fiabilité des résultats obtenues dans le chapitre précédent, afin de valider notre travail.

Chapitre1 : Généralité sur les réseaux informatiques

1.1 Introduction :

Les réseaux informatiques et Internet ont modifié notre façon de communiquer, d'apprendre, de travailler et de nous divertir. Les réseaux peuvent être de différentes tailles. Leur gamme s'étend des réseaux simples, constitués de deux ordinateurs, aux réseaux les plus complexes, capables de connecter des millions de équipements.

Au lieu de développer des systèmes uniques et distincts pour chaque nouveau service, le secteur du réseau dans son ensemble a adopté une structure de développement permettant aux développeurs de comprendre les plates-formes réseau actuelles et d'en assurer la maintenance. Parallèlement, cette structure permet de simplifier le développement de nouvelles technologies qui doivent répondre aux futurs besoins de communication et permettre des améliorations technologiques.

1.2 Définition d'un réseau informatique :

Le réseau informatique est l'ensemble des équipements (nœuds) reliés entre eux grâce à divers moyens matériels et logiciels pour échanger des données et partager des services. Qui va fournir le canal stable et fiable à travers lequel nos communications peuvent s'établir. L'infrastructure réseau se subdivise en deux parties [1]:

1.2.1 Le matériel :

Le matériel rassemble les périphériques (appareils) et les supports de transmission, qui correspond souvent aux composants visibles de la plate-forme réseau et on distingue :

a) Les périphériques finaux :

Ces périphériques forment l'interface entre les utilisateurs et le réseau de communication sous-jacent. Un périphérique final est la source ou la destination d'un message transmis sur le réseau, chaque périphérique final présent sur un réseau est identifié à l'aide d'une adresse. Parmi les périphériques finaux, on note : un ordinateur (station de travail, Serveur), Tablettes, téléphones VoIP.

b) Les périphériques réseau intermédiaires :

Les périphériques intermédiaires connectent les périphériques finaux au réseau et peuvent connecter plusieurs réseaux individuels afin de former un inter-réseau.

Les périphériques intermédiaires fournissent la connectivité et s'assurent que les données sont transmises sur le réseau. Ils utilisent l'adresse du périphérique final de destination, ainsi que les informations concernant les interconnexions réseau, pour déterminer le chemin que doivent emprunter les messages à travers le réseau. Des exemples des périphériques intermédiaires : les commutateurs, les routeurs, les points d'accès.

Et chaque périphérique sur le réseau a une carte réseau qui joue le rôle d'une interface entre lui et le réseau. La fonction d'une carte réseau est de préparer, d'envoyer et de contrôler les données sur le réseau.

c) Les supports de transmission :

Le support fournit le canal via lequel le message se déplace de la source vers la destination. Ceci est souvent effectué à travers une interface filaire par exemple fils métalliques ou fibre optique. L'interface air peut également être exploitée, à travers des communications non filaires, en utilisant l'infrarouge, le laser ou les ondes radio.

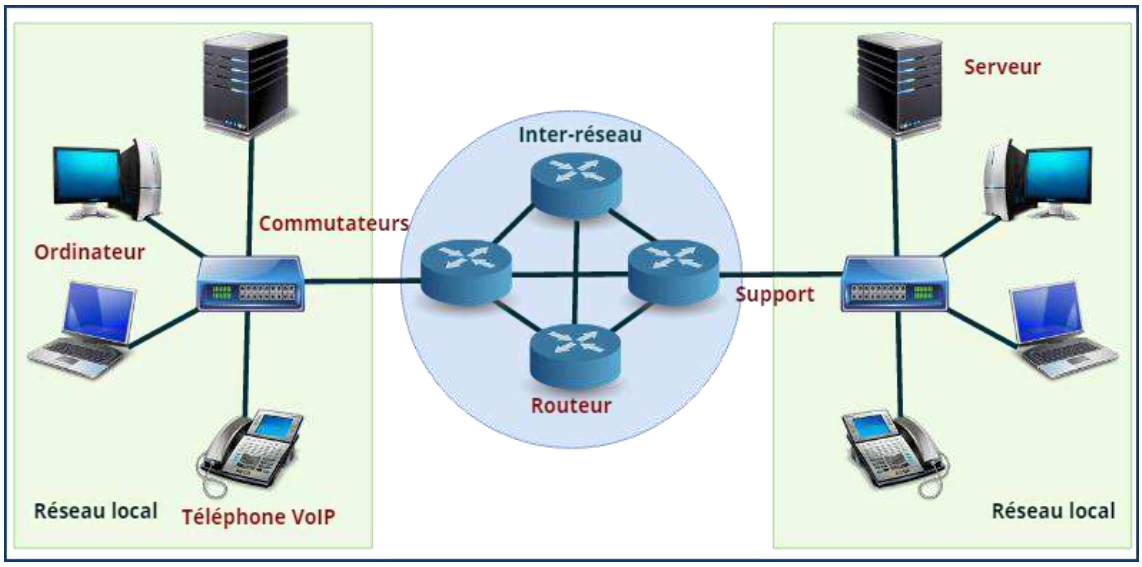

Figure 1. 1: Exemple d'un réseau informatique.

1.2.2 Logiciel :

Un logiciel est un ensemble de séquences d'instructions interprétables par une machine et d'un jeu de données nécessaires à ces opérations.

Le logiciel détermine donc les taches qui peuvent être effectuées par la machine, ordonne son fonctionnement et lui procure ainsi son utilité fonctionnelle, les séquences d'instructions appelées programme ainsi que les données du logiciel sont ordinairement structurées en fichiers, La mise en œuvre des instructions du logiciel est appelée exécution.

1.3 Classification des réseaux informatiques :

La classification des réseaux informatiques se fait selon leur étendue géographique de la manière suivante [figure 1.2] [2] :

- **Le réseau local LAN (Local Area Network) :** le LAN relie des utilisateurs et des périphériques finaux dans une zone géographique peu étendue quelques dizaines à quelques centaines de mètres, il s'agit généralement d'un réseau de petite ou moyenne entreprise ou d'un réseau domestique.
- **Le réseau métropolitain MAN (Metropolitan Area Network) :** le MAN permet l'interconnexion de plusieurs réseaux LAN dans une zone urbaine (ville, campus), par des liaisons privée ou publique.
- **Le réseau étendu WAN (Wide Area Network):** Le WAN relie des LAN ou des MAN sur des zones étendues couvrant des pays, des continents ou la planète toute entière, les réseaux étendus sont généralement gérés par des prestataires de services ou des fournisseurs d'accès à Internet (FAI). Le WAN le plus célèbre est le réseau public Internet.

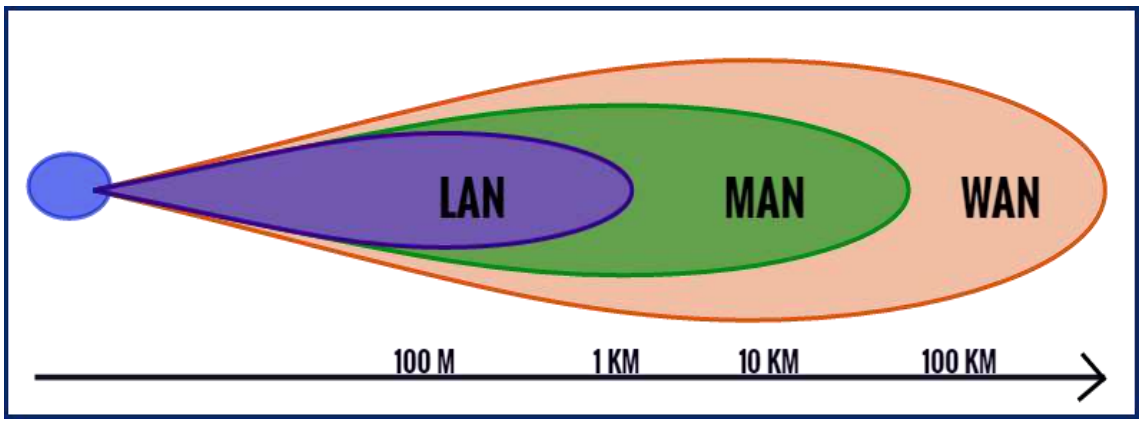

Figure 1. 2: Classification des réseaux informatiques.

- **Le réseau Internet :** Internet est le plus grand réseau existant. En réalité, le terme « Internet » signifie « réseau de réseaux ». Internet est littéralement un ensemble de réseaux privés et publics interconnectés. Grâce au réseau internet, nous sommes plus connectés que jamais.

  Il existe plusieurs manières de connecter des utilisateurs et des entreprises à Internet, les utilisateurs ont généralement besoin d'un fournisseur d'accès à Internet (FAI) pour se connecter à Internet. Les options de connexion varient considérablement d'un FAI et d'une région à l'autre. Cependant, les options les plus utilisées sont le câble haut débit, la technologie DSL (Digital Subscriber Line) haut débit, les WAN sans fil et les services mobiles [1].

1.4 Les architecteurs des réseaux informatiques :

a) Réseau client-serveur :

Un réseau client-serveur [figure 1.3] c'est un réseau qui utilise un ordinateur central pour délivrer des informations et des ressources au pré des autres périphériques finaux de réseau. L'ordinateur central est appelé un serveur, les serveurs sont des ordinateurs équipés de logiciels leur permettant de fournir des informations, comme des messages électroniques ou des pages web, à d'autres périphériques finaux (les clients) sur le réseau. Les protocoles TCP, UDP, FTP, POP, IMAP et SMTP fonctionnent en mode client-serveur [2].

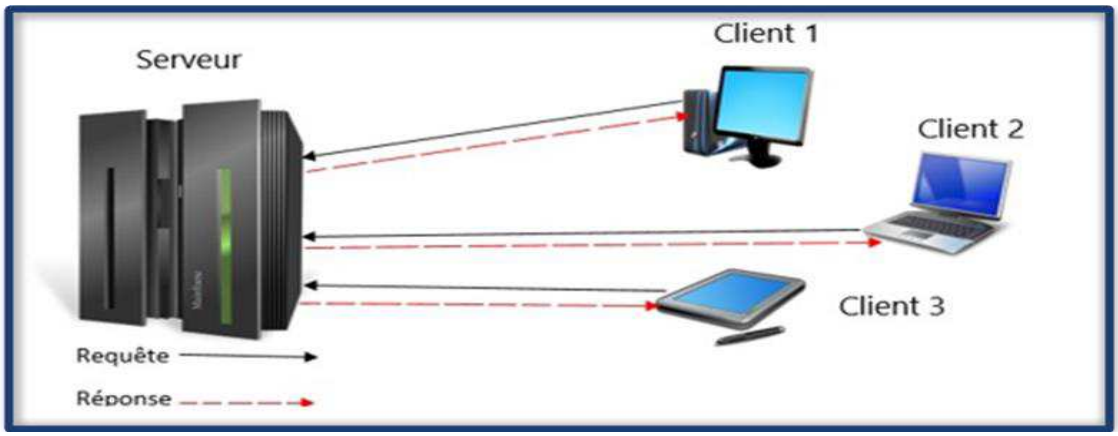

Figure 1. 3: Réseau client-serveur.

d) Réseau point à point (peer to peer) :

Dans un réseau point à point [figure 1.4] les postes ont un rôle identique et ils sont à la fois clients pour des ressources et serveurs pour d'autres. Dans ce type de structure,

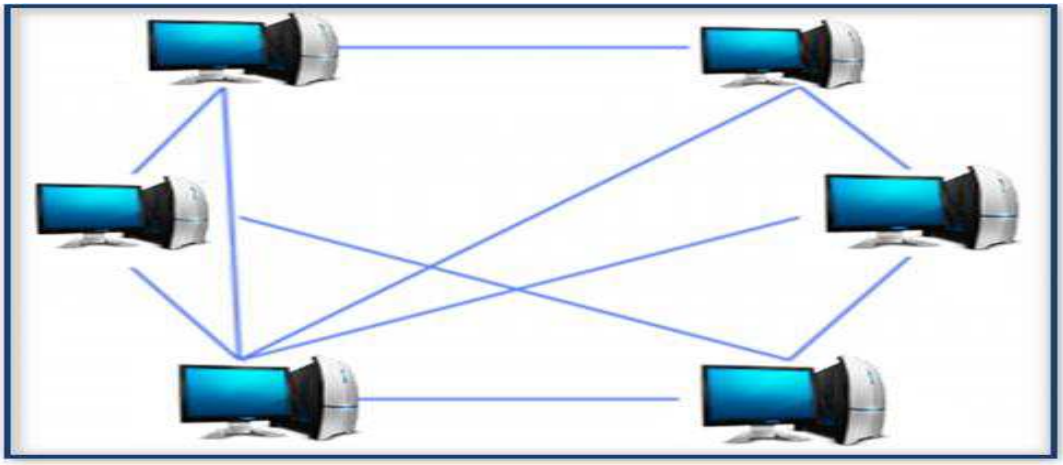

Figure 1. 4: Réseau point à point.

regroupant en général peu de postes, les ressources, les opérations de sécurité, les tâches d'administration sont réparties sur l'ensemble du réseau. Le contrôle centralisé est donc rendu impossible. Chaque utilisateur est souvent administrateur de son propre poste [1].

1.5 Les topologies des réseaux informatiques :

1.5.1 Topologie physique :

Une topologie physique relative au plan du réseau qui désigne les connexions physiques. Les périphériques peuvent être interconnectés selon les topologies physiques suivantes [3] :

- **Topologie en bus :** la plus ancienne topologie existante, le réseau en bus repose sur un câblage unique sur lequel viennent se connecter des périphériques, avec une liaison passive par dérivation.
- **Topologie en étoile :** est la topologie la plus utilisée de nos jours, dans le réseau en étoile les périphériques finaux sont connectés à un périphérique intermédiaire central (commutateurs Ethernet). La topologie en étoile est simple à installer, très évolutive et facile à dépanner.
- **Topologie en anneau :** dans la topologie en anneau les périphériques finaux sont connectés à leur voisin respectif et forment ainsi un anneau et chaque station est

connectée au support par un port d'entrée et elle transmet les données à la station suivante par son port de sortie.

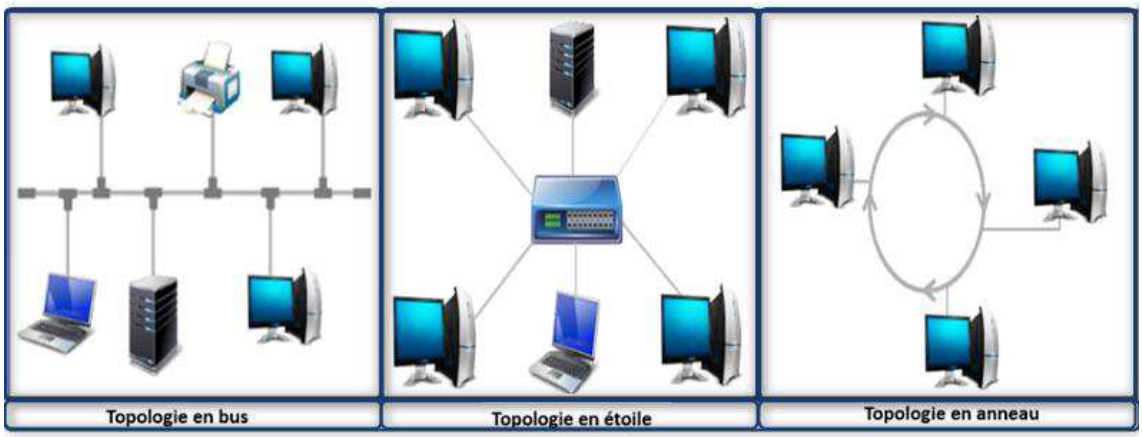

Figure 1.5: Les topologies physiques des réseaux informatiques.

1.5.2 Topologie logique :

Les topologies logiques définissent la manière dont les équipements échangent leurs données et nombreux aspects de la communication réseau dont le format et la taille des trames [4].

- **Ethernet :** Ethernet est désormais la technologie de réseau local prédominante dans le monde, est normalisée sous l'appellation 802.3 par L'IEEE. Il fonctionne au niveau de la couche physique et de la couche liaison de données, on peut avoir Ethernet sur différents réseaux câblés, les spécifications Ethernet prennent en charge différents supports, bandes passantes et codage de signal et le format de trame et le schéma d'adressage.
- **Token Ring :** Token Ring est une norme de réseau local et métropolitain, normalisé comme 802.5 par l'IEEE. Son but est de fournir une interconnexion compatible d'équipement de traitement de données au moyen d'un réseau local utilisant la méthode d'accès par passage de jeton dans les réseaux en anneau.
- **FDDI (Fiber Distributed Data Interface):** FDDI est une technologie de réseau MAN et LAN, normalisée par ISO sous le numéro 9314. FDDI est un réseau en anneau optique sur fibre optique multimode ou monomode. Le débit nominal est de 100 Mbit/s pour une distance maximale de 100 km.

1.6 Modèles OSI et TCP/IP :

1.6.1 Modèle TCP/IP :

Le modèle de protocole TCP/IP (Transmission Control Protocol/Internet Protocol) pour les communications inter-réseau, est appelé aussi modèle Internet parce qu'il est la source du réseau Internet. TCP/IP est un modèle en 4 couches qui décrit la fonctionnalité des protocoles qui constituent la suite de protocoles TCP/IP [1].

1.6.2 Modèle OSI :

Le modèle de référence OSI (Open Systems Interconnection) divise le processus de réseau en sept couches logiques et cela permet de visualiser plus facilement les mécanismes sous-jacents de la communication via le réseau.

Dans le modèle OSI, la couche d'accès réseau et la couche d'application du modèle TCP/IP sont subdivisées pour décrire les fonctions distinctes qui doivent intervenir sur ces couches. Les principales similitudes concernent les couches transport et couche réseau [figure 1.6].

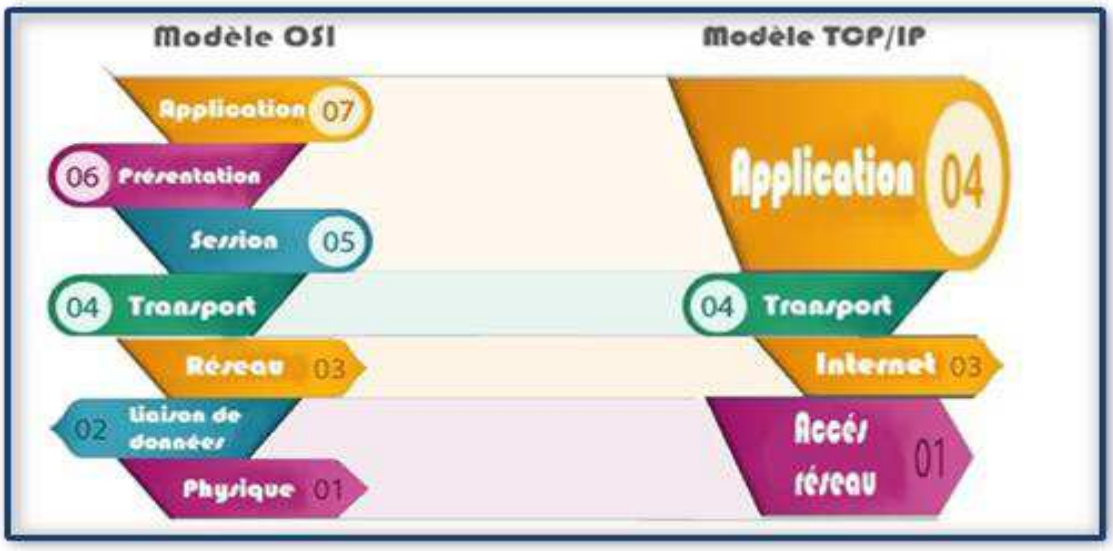

Figure 1. 6: Modèles OSI et TCP/IP.

1.6.3 Couche Accès réseau :

Couche accès réseau est responsable des trames émises et reçues et définits, et elle contrôle les périphériques matériels et les supports qui constituent le réseau.

Cette couche prépare les données à être placées sur les supports physiques en encapsulant le paquet des couches internet dans une trame. L'encapsulation consiste à ajouter les adresses

MAC, des processus d'accès au support et des informations de contrôle pour faciliter la transmission de la trame.

Au niveau de cette couche, les trames sont codées sous la forme d'une série de signaux électriques, optiques ou ondulatoires (radio).

Adresse MAC :

Une adresse MAC Ethernet est une valeur binaire de 48 bits constituée de 12 chiffres hexadécimaux et chaque interface réseau a une adresse MAC unique gravée dans la ROM de la carte réseau.

L'adressage MAC fournit une méthode d'échange des données sur des réseaux Ethernets et elle est utilisée par la carte réseau pour déterminer si un message doit être transmis à la couche supérieure en vue de son traitement. Les commutateurs (les switchs) de couche 2 effectuent la commutation et le filtrage basés uniquement sur l'adresse MAC [1].

Exemple d'une adresse MAC : 00-18-DE-DD-A7-B2.

1.6.4 Couche Internet :

Cette couche sert à décrire les protocoles qui traitent et dirigent les messages via l'inter-réseau donc elle s'occupe de l'adressage logique, de l'encapsulation des paquets de données et du routage et la désencapsulation.

a) Protocole IPv 4 :

IPv4 assure une livraison des paquets sans connexion et sans garantie et s'occupe de la structure, de l'adressage et du routage des paquets. Chaque nœud du réseau doit être identifié par une adresse IP unique sur le réseau.

b) L'adresse IPv4 :

Chaque adresse est une chaîne de 32 bits divisée en quatre parties appelées octets. Chaque octet contient 8 bits séparés par un point. Pour simplifier leur utilisation, les adresses IPv4 sont souvent exprimées en notation décimale à point, par exemple, l'adresse IPv4 d'un PC est : 192.168.10.10. Il y a deux types d'adresse IPv4, adresse IPv4 publique et privée [3].

Les adresses IPv4 publiques sont acheminées de manière globale entre les routeurs des FAI (fournisseurs d'accès à Internet) et ils sont attribuées par ce dernier. Certaines plages

d'adresses appelées adresses privées sont utilisées par la plupart des entreprises pour attribuer des adresses IPv4 aux hôtes dans leur réseau interne, ces adresses ne sont pas routables via internet et doivent être traduites en adresses IPv4 publiques à l'aide de la traduction NAT. Généralement cette opération s'effectue sur le routeur qui connecte le réseau interne à celui du FAI [4].

Classe	Plages d'adresses locales	Préfixe
A	10.0.0.0 – 10.255.255.255	10.0.0.0/8
B	172.16.0.0 – 172.31.255.255	172.16.0.0/12
C	192.168.0.0 – 192.168.255.255	192.168.0.0/16

Tableau 1.1 :Plage d'adresse local

c) Masque de sous-réseau :

Il sert à identifier la partie réseau et la partie hôte d'une adresse IPv4. Comme l'adresse IP est repérée sur 4 octets (32 bits), des masques simples peuvent être : 255.0.0.0, 255.255.0.0 ou 255.255.255.0 [1].

d) En-tête de paquet IPv4 :

Un en-tête de paquet IPv4 [figure 1.7] est constitué de champs contenant des informations importantes sur le paquet comme [1] :

- Version : ce champ a la valeur 0100 indiquant qu'il s'agit d'un paquet IP version 4.
- Services différenciés ou DiffServ (DS) : le champ Services est utilisé pour définir la priorité de chaque paquet.
- Time-to-live (durée de vie, TTL) : ce champ est utilisé pour limiter la durée de vie d'un paquet.
- Protocoles : ce champ indique le prochain protocole de couche supérieure à utiliser ensuite.
- Adresse IP source et destination : ces deux champs représentent l'adresse IP de source et destination du paquet.
- Les champs Longueur d'en-tête Internet (IHL), Longueur totale et Somme de contrôle d'en-tête permettent d'identifier et de valider le paquet.

- Les paquets IPv4 utilisent les champs Identification, Indicateurs et Décalage du fragment pour garder la trace des fragments.

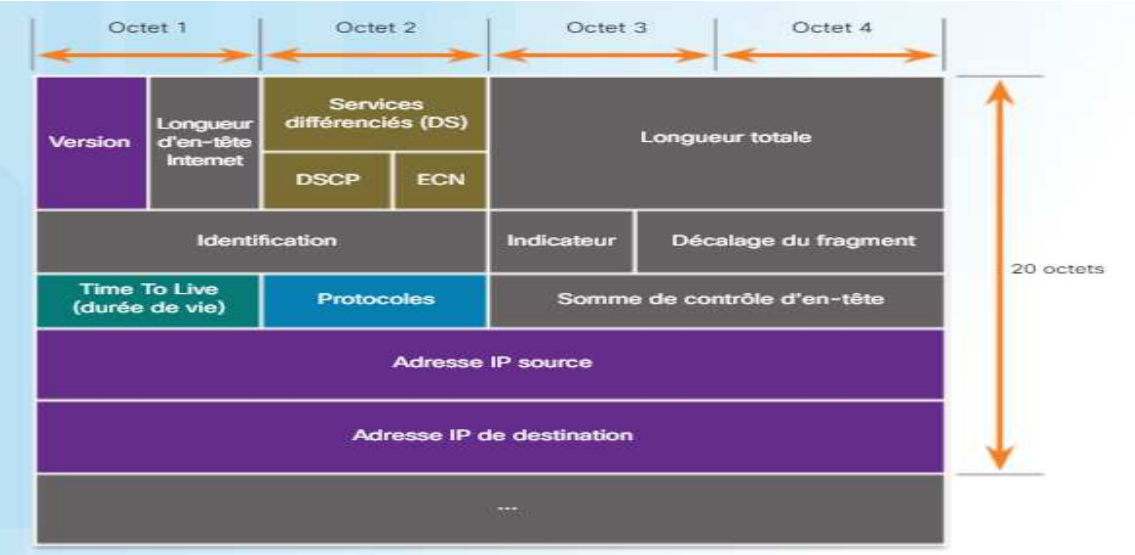

Figure 1. 7: En-tête de paquet IPv4 [1].

e) NAT (Network Address Translation) :

La traduction d'adresse réseau (NAT) assure la traduction des adresses privées en adresses publiques. La fonction NAT peut être utilisée à différents fins, mais son utilisation principale consiste à limiter la consommation des adresses IPv4 publiques. Ainsi, elle permet aux réseaux d'utiliser des adresses IPv4 privées en interne, et assure la traduction de ces adresses en une adresse publique lorsqu'il est nécessaire. La NAT permet d'ajouter un niveau de sécurité et de confidentialité au réseau en empêchant les réseaux externes de voir les adresses IPv4 internes [5].

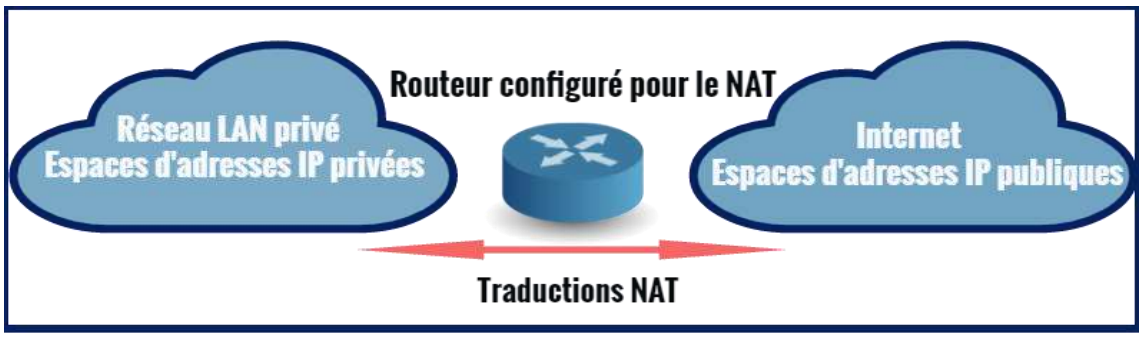

Figure 1. 8: Traductions NAT.

Les routeurs assurent la fonction NAT, ils peuvent être configurés avec plusieurs adresses IPv4 publiques (pool NAT) et les serveurs proxy assurent aussi la fonction NAT et ils sont utilisés dans les réseaux des grandes entreprises ou campus. La NAT qualifie également les adresses locales ou globales :

Adresse locale: L’adresse locale fait référence à toute adresse qui apparaît sur la partie interne du réseau.

Adresse globale : L’adresse globale fait référence à toute adresse qui apparaît sur la partie externe du réseau.

Fonctionnement de NAT :

Lorsqu'une machine du réseau effectue une requête vers Internet, la passerelle effectue la requête à sa place, reçoit la réponse, puis la transmet à la machine ayant fait la demande (une translation des paquets provenant du réseau interne vers le réseau externe).

La translation d’adresse se fait de deux manières :

1) **Translation statique :**

Le principe du NAT statique consiste à associer une adresse IP publique à une adresse IP privée interne au réseau. Le routeur (ou plus exactement la passerelle) permet donc d'associer à une adresse IP privée (par exemple 192.168.0.1) une adresse IP publique routable sur Internet et de faire la traduction, dans un sens comme dans l'autre, en modifiant l'adresse dans le paquet IP.

2) **Translation dynamique :**

Le NAT dynamique permet de partager une adresse IP routable (ou un nombre réduit d'adresses IP routables) entre plusieurs machines en adressage privé. Ainsi, toutes les machines du réseau interne possèdent virtuellement, vu de l'extérieur, la même adresse IP.

Afin de pouvoir « multiplexer » (partager) les différentes adresses IP sur une ou plusieurs adresses IP routables le NAT dynamique utilise le mécanisme de translation de port (PAT - Port Address Translation), c'est-à-dire l'affectation d'un port source différent à chaque requête de telle manière à pouvoir maintenir une correspondance entre les requêtes provenant du réseau interne et les réponses des machines sur Internet, toutes adressées à l'adresse IP du routeur.

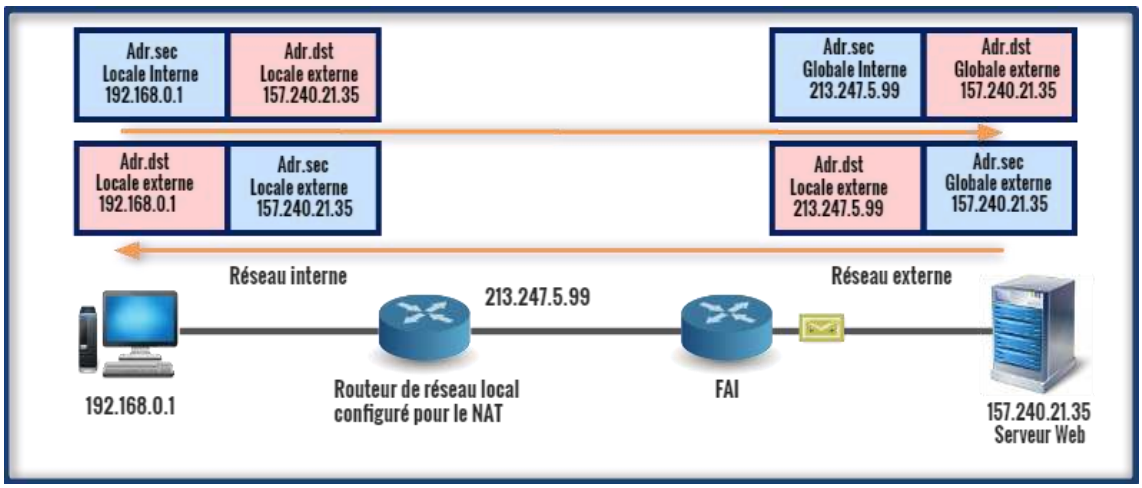

Figure 1. 9: Exemples de traduction d'adresse réseau.

1.6.5 Couche Transport :

La couche transport est chargée de l'établissement d'une session de communication temporaire entre deux applications et de l'acheminement des données entre ces deux applications et décrit les services et les fonctionnalités de base qui assurent l'ordre et la fiabilité de ces données. La suite de protocoles TCP/IP propose deux protocoles de couche transport, TCP et UDP.

a) Protocole TCP (Transmission Control Protocol):

Le protocole TCP est défini dans le but de fournir un service de transfert de données fiable en séquence d'un flux full-duplex. TCP est un protocole fiable de bout en bout, orienté connexion, ça veut dire un protocole qui négocie et établit une connexion permanente (mode connecté) entre les périphériques sources et de destination avant de transmettre du trafic. TCP est utilisé par ces applications nécessitant un service de transport fiable, par exemple, courrier (SMTP), Telnet, HTTP pour la navigation web [6].

1) En-tête TCP :

Dans l'en-tête TCP [figure 1.10] on trouve les éléments suivants :

- Port source et port de destination : utilisés pour identifier le numéro de port logique utilisé par l'application.
- Numéro d'ordre : utilisé pour réorganiser les données.
- Numéro d'accusé de réception : indique les données qui ont été reçues.

- Longueur d'en-tête : Indique la longueur de l'en-tête du segment TCP.
- Réservé : champ réservé pour les futures évolutions.
- Bits de contrôle : comprennent des codes de bits, ou indicateurs, indiquant l'objectif et la fonction du segment TCP.
- Taille de fenêtre : indique le nombre des segments pouvant être acceptés en même temps.
- Somme de contrôle : utilisée pour le contrôle des erreurs dans l'en-tête et les données du segment.
- Urgent : indique si les données sont urgentes.

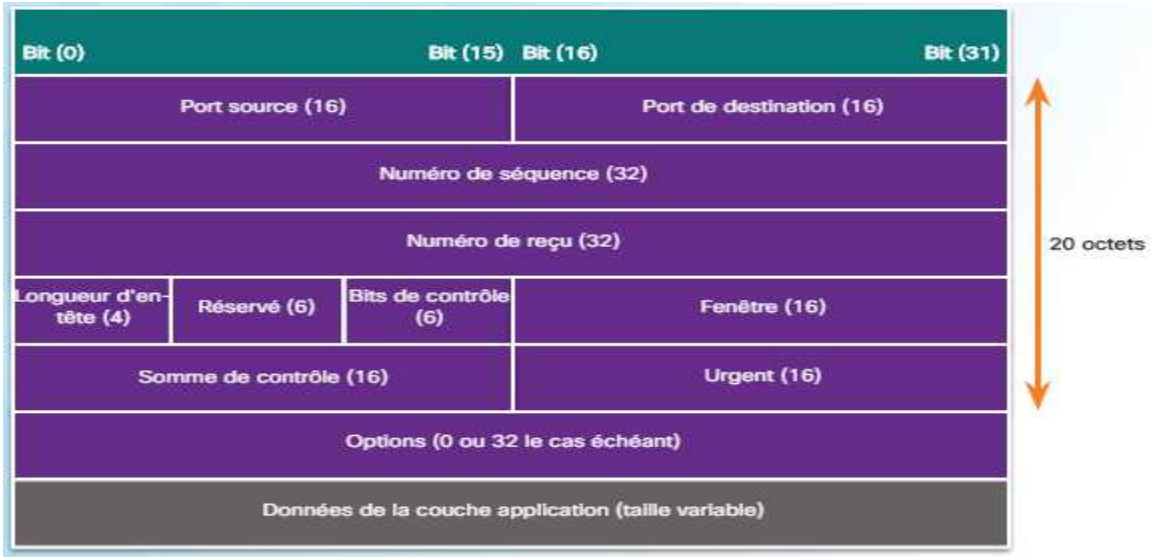

Figure 1. 10: En-tête TCP [1].

2) Les flags dans l'en-tête TCP :

Le flag dans un paquet TCP peut être positionné par l'attribution de la valeur 1 dans le champ de flag, on liste plusieurs flags dans le paquet TCP qui peuvent être présents :

- Flag SYN : le champ SYN est code sur 1 bit et indique la synchronisation des numéros de séquence.
- Flag ACK : le champ ACK est code sur 1bit et indique que le numéro de séquence pour les acquittements est valide.
- Flag PUSH : le champ PUSH est code sur 1 bit et indique au récepteur de délivrer les données à l'application et de ne pas attendre le remplissage des tampons.
- Flag FIN : le champ FIN est code sur 1 bit et indique fin de transmission.

- Flag URG : le champ URG est code sur 1 bit et indique que le champ pointeur de donnée urgente est utilisé, pour indiquer que ces donnes sont prioritaires.
- Flag RST : le champ RST est code sur 1 bit et demande la réinitialisation de la connexion.
- Le champ réservé : il contient 4 flags qui sont (réservé sur 3 bits, ECN/ns sur 1 bit, CWR 1 sur bit, ECE sur 1 bit), il servira pour des besoins futurs.

3) Les ports :

De nombreuses applications (programmes TCP/IP) peuvent être exécutées simultanément sur l'ordinateur (par exemple ouvrir plusieurs navigatrices simultanément ou bien naviguer sur des pages web et en télécharger un fichier).

L'ordinateur doit distinguer ces différentes applications afin de fournir correctement les données qui sont destinées à chaque application, afin de réaliser ce processus l'ordinateur va attribuer un numéro de port qui indique l'application à laquelle les données sont destinées, lorsque l'ordinateur reçoit des données destinées à un port, les données sont envoyées vers l'application correspondante.

Port source : le numéro du port source est génère de manière dynamique par le périphérique émetteur pour identifier une conversation entre deux périphériques.

Port destination : le client place un numéro de port de destination dans le segment pour informer le serveur de destination du service demandé, par exemple pour les services web le numéro de port spécifié est 80.

4) Établissement d'une connexion TCP

La "three-way handshake" ou "la connexion en trois étapes" est la procédure utilisée par le protocole TCP pour ouvrir une connexion entre deux hôtes (hôte A et hôte B) [7].

Le client ouvre la connexion en envoyant un premier segment, parfois appelé séquence de synchronisation. Ce segment contient en particulier le numéro de séquence initial (le numéro du premier octet émis) et le drapeau SYN est mis à 1.

Le serveur répond par un acquittement comprenant le numéro du premier octet attendu (celui qu'il a reçu + 1) et son propre numéro de séquence initial (pour référencer les octets de données du serveur vers le client). Dans ce segment de réponse, le serveur a positionné les drapeaux SYN et ACK à 1.

Enfin, le client acquitte la réponse du serveur en envoyant un numéro d'acquittement égal au numéro de séquence envoyé par le serveur + 1. Dans ce troisième message, seul le drapeau ACK est mis à 1. L'ensemble des trois segments correspond à l'ouverture de la connexion, illustrée à la [figure 11.1]. Ce mécanisme d'ouverture est appelé three-way-handshake (établissement en trois phases). Après la dernière phase, le transfert des données peut commencer.

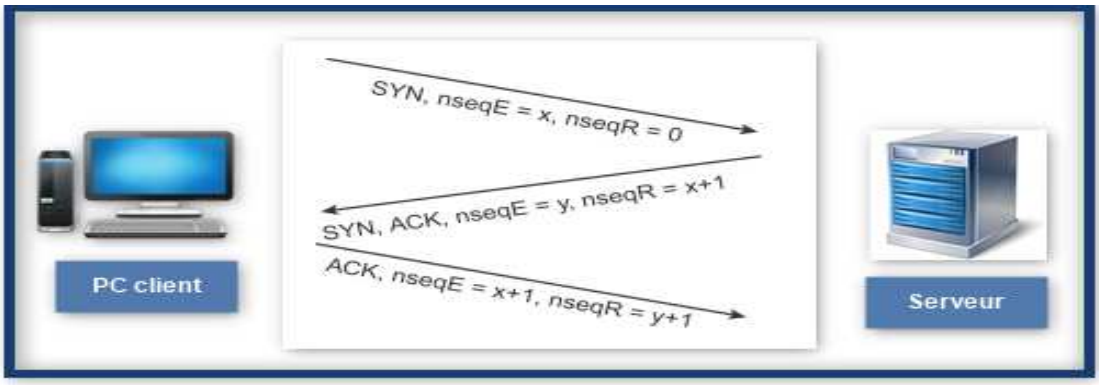

Figure 1.11 : Ouverture d'une connexion TCP.

b) Protocole UDP (User Datagram Protocol) :

UDP est un protocole de transport sans connexion qui permet l'émission des messages sans l'établissement préalable d'une connexion. C'est un protocole non fiable, beaucoup plus simple que TCP, car il n'ajoute aucune valeur ajoutée par rapport aux services offerts par IP. Il est utilisé pour les transmissions gourmandes, telles que la vidéo et le son (streaming, vidéo conférence) [7].

c) En-tête UDP :

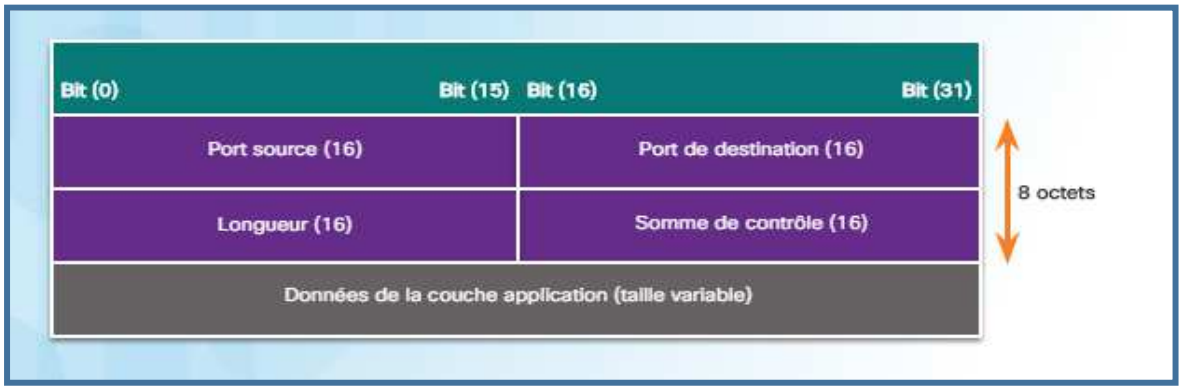

Figure 1. 12: En-tête UDP [1].

1.6.6 Couche Application :

La couche application TCP/IP inclut plusieurs protocoles qui fournissent des fonctionnalités spécifiques à plusieurs applications d'utilisateur final. Les protocoles de couche application sont utilisés pour échanger des données entre les programmes s'exécutant sur les hôtes sources et de destination.

1) Applications réseaux :

Les applications sont les programmes logiciels qui permettent aux utilisateurs de communiquer sur le réseau. Les clients de messagerie et les navigateurs Web sont des exemples de ces types d'applications.

Un navigateur web (browser) : est un logiciel destiné à la consultation des ressources du World Wide Web, les sites web, notamment les pages au format HTML. En pratique, le navigateur nous traduit en texte, image, vidéo les pages d'information qui sont codées en HTML. Le navigateur web nous permet de naviguer sur internet, consulter des sites web et télécharger des fichiers.

Protocoles de couche Application :

Les protocoles de couche application sont utilisés par les périphériques source et de destination pendant une session de communication. Les protocoles de couche application les plus utilisés sont :

- **DNS (Domain Name System) :** c'est un service ou système utilisé pour traduire les noms de domaine Internet en adresse IP.
- **DHCP (Dynamic Host Configuration Protocol) :** attribue dynamiquement des adresses IP aux stations clients .
- **SMTP (Simple Mail Protocol Protocol) :** POP (Post Office Protocol), IMAP (Internet Message Access Protocol) : sont des protocoles du serveur de messagerie
- **FTP (File Transfer Protocol) :** a été développé pour permettre le transfert des fichiers entre deux hôtes.
- **HTTP (Hypertext Transfer Protocol) :** ensemble des règles permettant d'échanger des textes, des graphiques, des sons, des vidéos et autres fichiers multimédia sur le Web.

1.7 Proxy :

Un serveur proxy (serveur mandataire) est une machine, généralement un ordinateur, qui fait le rôle d'un intermédiaire entre les machines d'un réseau local et internet. Sur internet, il existe différents types de proxy, les plus courants sont les proxys http. Ils supportent les protocoles http et FTP.

1.7.1 Fonctionnement d'un serveur proxy :

Il s'agit d'un serveur mandaté par une application pour effectuer les requêtes sur internet à la place des ordinateurs de réseau qui l'utilisent donc il assure la fonction NAT.

Lorsqu'un utilisateur se connecte à internet à l'aide d'une application cliente, configure pour utiliser un serveur proxy, celle-ci va se connecter en premier lieu au serveur proxy et lui donne sa requête et lui demande d'effectuer cette requête. Le serveur proxy va se connecter au serveur que l'application cliente cherche à rejoindre et lui transmet la requête. Le serveur va ensuite donner sa réponse au proxy, qui va à son tour la transmettre à l'application cliente.

1.7.2 Proxy-cache :

La plupart des proxys ont la fonction cache qui est la capacité à garder en mémoire les pages les plus souvent visitées par les utilisateurs du réseau local, afin de pouvoir les leur fournir le plus rapidement possible.

1.7.3 L'utilité d'un proxy en entreprise :

Un serveur proxy est indispensable dans un réseau d'entreprise, il permet d'accélérer la navigation sur internet par mettre en cache les pages web les plus demandées, ainsi il sert à cacher les adresses IP des utilisateurs du réseau d'entreprise et il peut supprimer les cookies, les pubs, les bananiers, les scriptes.

L'intérêt majeur d'un serveur proxy est dans le cadre de la sécurité informatique, en filtrant l'ensemble des connexions de l'entreprise à internet en analysant les requêtes clients et les réponses des serveurs en tenant compte de certaines critères (liste des adresses blanches, Liste des adresses noires, mots-clés, protocoles …).

Enfin, on peut utiliser un proxy pour authentifier les utilisateurs, afin de limiter l'accès au réseau internet, on donne l'accès aux ressources externes seulement aux personnes autorisées à le faire et l'enregistrer dans les fichiers journaux des accès identifies, ils se sentent suivis et restants sages dans leurs recherches.

Conclusion :

Dans ce chapitre, on a présenté les notions de base sur les réseaux informatiques, ensuite on a exposé les deux modèles principaux (OSI et TCP/IP) utilisés pour classifier et ordonner les protocoles et les standards de communication entre les machines.

Tout d'abord nous voulons, dans un premier temps, dans le chapitre, numéro 2 expliquer cette notion de vie privée sur internet, par une synthèse des différents systèmes et protocoles qui permettant de sécuriser et assurer l'anonymat des échangés sur internet.

Chapitre2: L'anonymat et la vie privée

2.1 Introduction :

Le web d'aujourd'hui n'est plus pensé comme une collection de sites à visiter, mais comme une plateforme permettant l'échange entre les utilisateurs, où ces derniers peuvent devenir actifs, participer, voir, écrire et s'exprimer librement. Aujourd'hui, presque tout ce qu'on fait sur Internet laisse une empreinte numérique qui décrit nos activités et précise leurs emplacements. Désormais, nous devons être prudents, car cet océan d'empreintes nous décrit d'une manière complète et avec un réalisme effrayant, d'où survient la question de l'anonymat et la protection de la vie privée en ligne.

Chacun a droit au respect de sa vie privée et l'anonymat est le moyen de préserver et protéger celle-là. L'anonymat en ligne est un concept essentiel de la protection de la liberté d'expression tout en permettant de se sentir en sécurité, de pouvoir surfer sur le web sans conséquences, de contourner les censures et les restrictions et éviter toutes sortes de plans publicitaires sur le web. Pour être anonyme sur le net, l'utilisateur a besoin de méthodes à la fois sécurisées, fiables et économiques, il est possible d'agir de différentes façons pour minimiser les traces qu'on laisse sur Internet. En exploitant l'option de navigation privée, en utilisant un proxy, en installant un VPN, en optant pour le projet Tor et son navigateur anonyme. Toutes ces méthodes bien sûr, présentent des avantages et des inconvénients, quelle que soit leur efficacité.

Toutefois, l'anonymat présente aussi des inconvénients : il peut être utilisé par des individus mal intentionnés dans des activités criminelles ou d'autres types d'actes répréhensibles tels que le harcèlement ou les intimidations en ligne.

2.2 L'anonymat et la vie privée :

L'anonymat reflète tout ce qui est non identifiable, se dit aussi de quelqu'un dont on ignore son adresse et ces coordonnées. Dans sa forme la plus simple, l'anonymat est le fait de ne pas être identifiable. Dans notre travail, on s'intéresse à l'anonymat en ligne.

Anonymat et vie privée sont très souvent associés, et pour cause, le premier est un moyen de préserver et protéger la seconde. La protection de la vie privée est d'empêcher une organisation, un gouvernement ou quiconque d'avoir accès à des informations, des données ou des affaires à caractère personnel. Chacun a droit au respect de sa vie privée tel qu'énonce dans l'article 12 de la Déclaration universelle des droits de l'homme des Nations Unies et la protection de l'anonymat en ligne a été liée à la protection du droit au respect de la vie privée [9].

2.3 L'intérêt de l'anonymat sur Internet:

L'anonymat permet à des individus de s'exprimer sans crainte de représailles et d'échapper aux surveillances en ligne, et il est particulièrement important dans les pays où la liberté d'expression est lourdement censurée et sanctionnée. Même dans les pays considérés comme démocratiques, la vie privée peut ne pas être respectée. Ceci est prouvé par la révélation d'Edward Snowden qui démontre que la NSA « Agence nationale de la sécurité » a effectué des collectes massives d'informations privées concernant les citoyens du monde entier et en particulier les présidents de plusieurs pays européens en les mettant sur écoute. Ceci dépasse le cadre de la lutte nécessaire contre le terrorisme et les autres risques géopolitiques [8].

Toutefois, ne sont pas uniquement les états unis qui procèdent à ce genre d'investigations. D'autres pays du monde aussi obligent leurs fournisseurs d'accès internet à surveiller les données et enregistrer les détails de connexion comme leur date, leur durée, leurs adresses IP et aussi les recherches web effectuées, les mails indiqués, et l'historique du navigateur.

Même les entreprises web privées et les réseaux sociaux conservent les données de leurs clients. D'ailleurs l'exemple le plus flagrant est le gigantesque moteur de recherche Google avec tous les services associés comme son fournisseur de mail Gmail qui possède des informations immenses sur leurs utilisateurs, malgré que ces données peuvent être fuiter ou partager avec d'autres organismes. Plus récemment, le scandale de "Cambridge Analytica" avec l'aide de Facebook a été divulgué. Il concernait l'utilisation de données personnelles de citoyens américains avant l'élection présidentielle de 2016 avec pour but d'orienter leur vote en faveur de Donald Trump.

Le deuxième argument pour l'anonymat est celui de ne pas être tracé par les entreprises commerciales qui ont une présence sur internet. Ces entreprises peuvent enregistrer à l'aide de "trackers" sous la forme de cookies flash les habitudes des utilisateurs et ainsi orienter leur publicité sur les navigateurs web de ces derniers.

Quelque fois, l'anonymat est utilisé pour se protéger contre les tentatives de piratage (sur carte bleue par exemple) ou d'autre forme de criminalité en ligne (comme la diffusion des données personnelles ayant pour but le chantage).

Comme tout autre système, l'anonymat possède un côté sombre. Elle peut être utilisée par des individus mal intentionnés dans des activités criminelles ou d'autres types d'actes répréhensibles tels que le téléchargement illégal, le harcèlement ou les intimidations en ligne et d'autres formes de criminalité.

2.4 Cryptage des données :

2.4.1 Définition :

Cryptographie est étymologiquement « écriture secrète ». C'est l'étude des techniques et des pratiques de chiffrement qui assurent l'inviolabilité des textes et des données et le chiffrement est l'opération qui consiste à transformer, à l'aide d'une clé, une donnée en clair (dite donnée claire) en une donnée incompréhensible (dite donnée chiffrée), qui ne peut être lue que par son créateur et son destinataire. Le chiffrement est utilisé pour la sécurisation de l'information et la protection des données lors de leur transfert sur le réseau.

Figure 2. 1: Fonction de chiffrement.

Cryptographie symétrique : (également dite à clé secrète), c'est la plus ancienne forme de chiffrement. Elle permet à la fois de chiffrer et déchiffrer des messages à l'aide d'une même clé, et l'AES est l'un des algorithmes de chiffrement symétrique.

Cryptographie asymétrique : (ou cryptographie à clé publique), c'est une méthode de chiffrement qui s'oppose à la cryptographie symétrique. Elle repose sur l'utilisation d'une clé

publique (qui est diffusé) et d'une clé privée (gardée secrète). La première permet de chiffrer le message et l'autre de le déchiffrer, et l'RSA est l'un des algorithmes de chiffrement asymétrique.

Le hache : est une représentation minime de données qui marche dans un sens unique, ce que veut dire qu'on ne peut pas récupérer les données initiales à partir du hache. Il est utilisé pour vérifie l'intégralité des données au décryptage.

2.4.2 SSL et TLS :

SSL (Secure Sockets Layer) : Historiquement créé dans les années 90 par la société Netscape, il a été repéré après par L'IETF pour rendre le protocole plus ouvert et plus standardisé et aussi pour éviter les problèmes de droit, ils ont décidé de renommer le protocole et de l'appeler TLS (Transport Layer Security). On parle parfois de SSL/TLS pour désigner indifféremment SSL ou TLS.

SSL/TLS sont des protocoles de sécurisation des échanges sur internet. Ils sont utilisés pour apporter plusieurs fonctions de sécurité lors de l'échange de données. SSL/TLS fonctionnent suivant un mode client-serveur avec l'interdiction d'une nouvelle couche de communication entre celle du transport et celle d'application du modèle TCP/IP dédié à la sécurité.

2.4.3 Fonctionnement de SSL/TLS :

Avant d'expliquer le fonctionnement de TLS, il est important de faire un point sur l'état actuel des choses et comprendre pourquoi on a besoin de cette couche de sécurité supplémentaire.

Sans SSL/TLS, les informations sont envoyées en clair lors d'un échange entre un client et un serveur. Le problème est que si quelqu'un se connecte au réseau, il lui serait facile d'intercepter les données échangées (Sniffing attack) et récupérer des informations. L'autre problème qu'on peut rencontrer est si quelqu'un pourrait faire semblant de se mettre à la place de serveur de destination (Phishing attack), alors il pourrait facilement faire croire à la victime qu'elle s'adresse à un tiers de confiance. Afin de lui soutirer des renseignements personnels : mot de passe, numéro de carte de crédit.

Donc l'enjeu de SSL/TLS est double. D'une part, il permet de chiffrer les informations échangées entre le client et le serveur, et de l'autre, une authentification et de s'assurer que l'ordinateur avec lequel on communique est bien celui qu'on prétend.

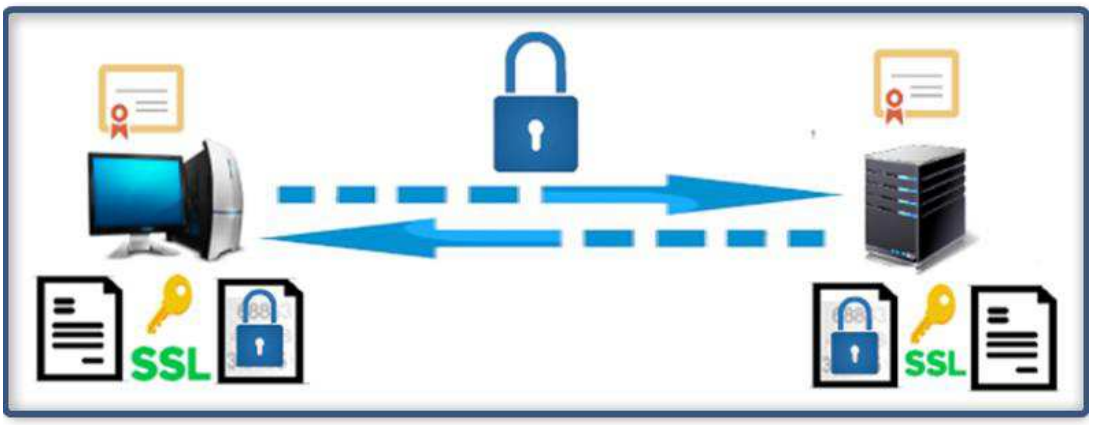

Figure 2. 2:Fonctionnement de SSL/TLS.

2.4.4 Certificat SSL :

L'établissement d'une connexion SSL nécessite l'installation d'un certificat numérique sur le serveur Web. Ce certificat utilise alors les clés publiques et privées pour le cryptage, et identifie le serveur de manière unique et définitive. Les certificats numériques s'apparentent à une forme de carte d'identité électronique qui permet au client d'authentifier le serveur avant l'établissement d'un canal de communication crypté [10].

Un certificat SSL est délivré par une tierce partie de confiance, appelée Autorité de Certification (Certification Authority, ou CA). L'Autorité de Certification agit en quelque sorte comme une Préfecture ou une Mairie qui délivre des cartes d'identité : l'Autorité de Certification engage une série de vérifications selon des règles très strictes, afin d'établir avec certitude l'identité de l'entreprise et du serveur web; l'Autorité de Certification émet alors le certificat SSL et le retourne à l'administrateur du site web certifié [11].

2.4.5 Protocoles de SSL/TLS :

SSL/TLS utilise plusieurs protocoles pour la protection et la mise en place de la session sécurisée :

a) SSL handshake :

Le premier protocole « SSL handshake » permet l'échange des paramètres de sécurité (nombres aléatoires, liste des algorithmes). Il permet aussi l'authentification des deux communicateurs. Cependant, dans la plupart des cas, le serveur est uniquement authentifié. Ce protocole fait intervenir les échanges suivants entre le client et le serveur [figure 2. 3] [13]:

1. Le client envoie un message "Client bonjour" au serveur, ainsi que la valeur aléatoire du client et les suites de chiffrement prises en charge.

2. Le serveur répond en envoyant un message "Server hello" au client, avec la valeur aléatoire du serveur.

3. Le serveur envoie un message « Certificate », qui contient en particulier sa clé publique au sein d'un certificat numérique.

4. Après validation du certificat et vérification de la signature précédente, le client crée un secret pré-maître aléatoire et le crypte avec la clé publique extraite du certificat du serveur, ensuit il envoie le secret pré-maître crypté au serveur.

5. Le serveur reçoit le secret pré-maître. Le serveur et le client génèrent chacun de son côté le secret maître et les clés de session (clé de hachage et clé écriture) en fonction du secret pré-maître.

6. Le client signale l'adoption du secret maître et les clés de session avec un ''ChangeCipherSpec''. Le client envoie également le message " Client finished ".

7. Le serveur reçoit "Change cipher spec", ensuit il envoie un message " Client finished " au client.

8. Le client et le serveur peuvent maintenant échanger des données d'application sur le canal sécurisé qu'ils ont établi. Tous les messages envoyés du client au serveur et du serveur au client sont chiffrés à l'aide de la clé de session.

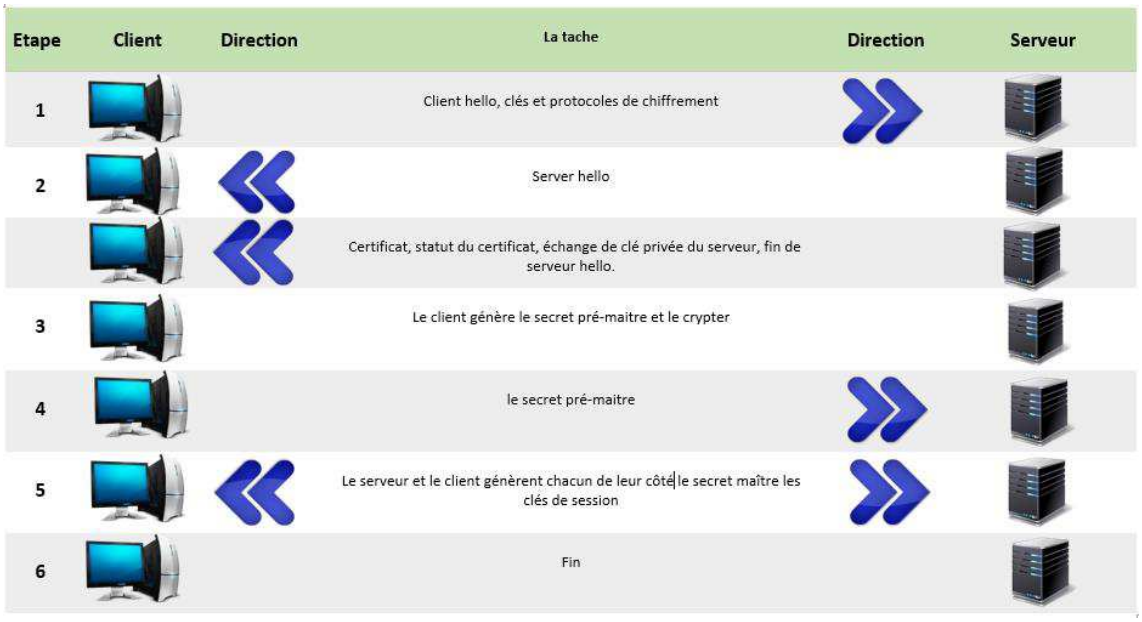

Figure 2. 3: Les étapes de TLS handshake.

b) SSL change Cliper Spec Protocol :

Le deuxième protocole « SSL change Cliper Spec Protocol » est utilisé pour indiquer un changement dans les algorithmes de chiffrement cryptographique, immédiatement après le changement toutes les données sont cryptées avec le nouveau chiffrement sélectionné.

c) SSL Alert Protocol :

Le troisième protocole « SSL Alert Protocol » est responsable de la signalisation des problèmes dans la session SSL.

d) SSL Record Layer Protocol

Le dernier protocole « SSL Record Layer Protocol » une fois négocier ce protocole chiffre toutes les informations échanger et effectuer divers contrôles.

2.5 Les outils d'anonymat en ligne :

2.5.1 Les navigateurs privés :

Un des premiers outils qui vient à l'esprit de beaucoup gens, lorsqu'on parle d'anonymat sur internet est la navigation privée, une fonctionnalité désormais présente dans la quasi-totalité des navigateurs grands publique. Avant toute chose, il faut savoir que cette

fonctionnalité ne garantit pas l'anonymat sur Internet. Les fournisseurs d'accès à Internet, les employeurs ou les sites visités eux-mêmes pourront toujours nous pister, ou accéder à notre adresse IP.

En revanche les navigateurs privés proposent plusieurs fonctionnalités intéressantes. Lorsqu'on passe en mode navigation privée, plusieurs types de données ne sont plus enregistrés : l'historique de navigation, les cookies, les informations saisies dans les formulaires (mot de passe, adresse mail …), listes de téléchargements, les contenus mis en cache.

Pour ouvrir une fenêtre privée vide dans la plupart des navigateurs on clique sur le bouton ''menu'' puis sur ''nouvelle fenêtre de navigation privée''.

2.5.2 Proxy web :

a) Fonctionnement d'un Proxy web :

Proxy web a les mêmes fonctionnalités d'un serveur Proxy que nous avons expliqué dans le premier chapitre, d'une façon générale, il fonctionne comme un pont entre l'ordinateur de l'utilisateur et un site web, tout le trafic de l'utilisateur passe d'abord par le Proxy avant d'atteindre sa destination finale. L'utilisation d'un Proxy permet à la fois de masquer l'adresse IP de l'utilisateur donc surfer sur Internet de manière anonyme et de contourner la censure et les géo-restrictions (contenu limité géographiquement) et d'accéder à des sites bloqués.

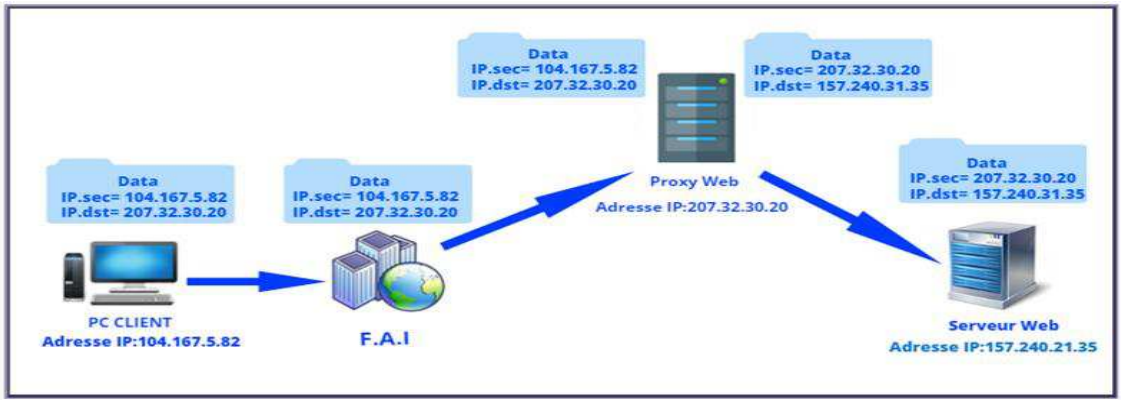

Figure 2. 4:Fonctionnement de Proxy Web.

b) L'inconvénient du Proxy web sur l'anonymat :

Le service Proxy web n'a pas vocation à nous rendre complètement anonymes sur le web par ce qu'en bas un serveur Proxy n'a pas la capacité de cryptage de données donc les données peuvent être interceptées, malgré que dans nos jours il y a plusieurs serveurs Proxy qui

proposent des services en HTTPs, mais on n'obtient pas la même protection qu'un bon VPN peut offrir [14].

c) Proxy web en pratique :

Il y a deux manières d'accéder à un service proxy, la première via une page web (proxy site web) dans laquelle il est possible de saisir une autre adresse, celle à laquelle on veut accéder à travers le proxy. Il y a plusieurs sites web qui propose ce service comme : proxysite.com, whoer.net.

Figure 2. 5: Exemple d'un Proxy page web (Proxysite.com).

La deuxième, on utilise le proxy « HTTP » ou « SOCKS » donc le proxy est accessible en modifiant les paramètres de connexion de l'application (par exemple le navigateur) il faut alors y renseigner l'adresse IP et numéro de ports du proxy. Il y a plusieurs sites web qui propose une liste d'adresse IP des saveurs Proxy comme : sslproxies.org, freeproxylists.net.

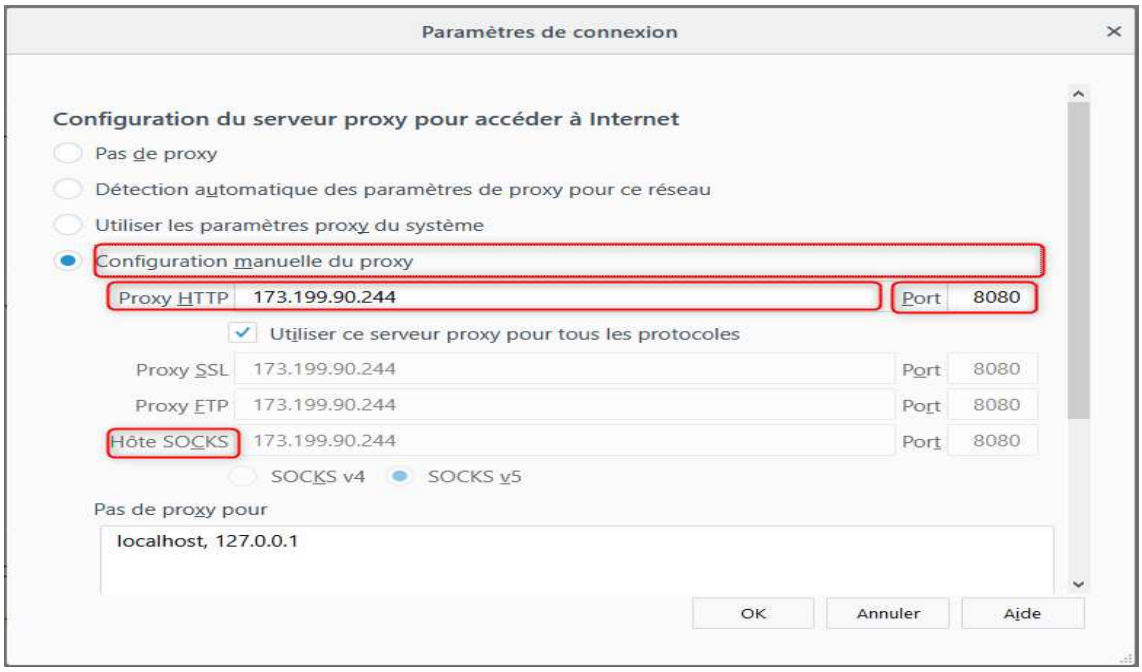

Figure 2. 6:Configuration du proxy sur navigateur web Mozilla Firefox.

SOCKS est un protocole internet qui permet l'échange de paquets réseaux entre un client et un serveur à travers un serveur proxy [15].

2.5.3 VPN :

VPN signifie Virtual Private Network (en français Réseau Privé Virtuel) appelé également « Tunnels », cela désigne un système permettant de crée un lien direct et sécurisé entre deux machines une sorte de tunnel de communication isolé des autres liens qui transitent sur cette liaison en général sur un réseau public. Les VPN peuvent utiliser des technologies et des protocoles quelconques et ils sont utilisés généralement pour protéger un trafic web privé contre les interférences, l'espionnage ou la censure, et de navigue sur le net de façon anonyme et privée.

a) Fonctionnement d'un VPN :

Le VPN repose sur un ou des protocoles de tunnellisation (Tunneling Protocols) comme : IPSec, PPTP,L2TP. Ils sont des protocoles permettent de chiffrer le paquet IP d'origine par des algorithmes de chiffrage, puis l'ajoutent un champ supplémentaire AH (Authentication Header) permettant à la réception de vérifier l'authenticité des données incluses dans le datagramme, en suite l'encapsulé dans un nouveau paquet IP avec un nouvel en-tête IP avant de l'envoyer sur le réseau [16].

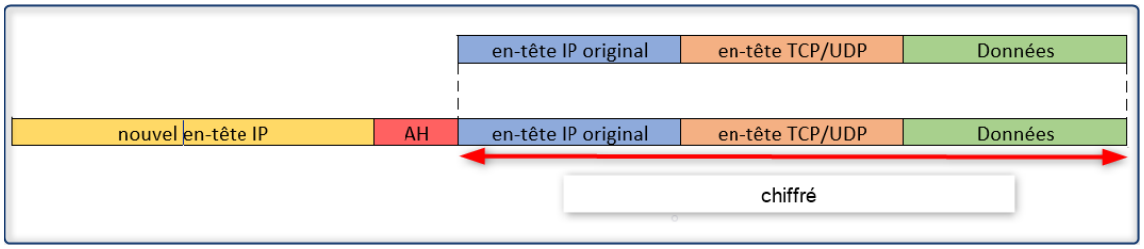

Figure 2. 7:L'encapsulation VPN.

On utilise d'ailleurs le terme de « tunnel » pour mettre l'accent sur le fait qu'entre l'entrée et la sortie d'un VPN les données sont chiffrées et protégées. Lorsqu'un VPN est établi entre deux réseaux physiques, l'élément qui permet de chiffrer et de déchiffrer les données du côté client (ou utilisateur) est nommé « Client VPN ». On appelle « Serveur VPN » l'élément qui chiffre et qui déchiffre les données du côté de l'organisation.

b) VPN d'entreprise :

Les VPN d'entreprise, qui forment le réseau logique d'interconnexion de plusieurs sites d'une entreprise, permettent en outre à des utilisateurs hors des sites de se connecter sur ce réseau logique et d'accéder aux données de l'entreprise en toute sécurité. Bien qu'il soit nécessaire de mentionner cet avantage, le réseau privé d'entreprise n'est pas vraiment le sujet de ce chapitre.

c) VPN internet :

Le VPN internet est un système consistant en l'usage d'un serveur proposé par un fournisseur VPN pour se connecter à Internet et c'est un VPN à vocation commerciale.

Ce VPN protège la confidentialité en linge puisqu'il peut agir en tant que proxy en masquant l'adresse IP d'origine par l'adresse du VPN ce que permet de masquer la localisation et de contourner la censure.

VPN propose des algorithmes de chiffrage haut niveau ce que permet d'avoir des données entièrement chiffrées entre le client et le serveur VPN donc incompréhensibles pour toute personne située entre les deux extrémités du VPN.

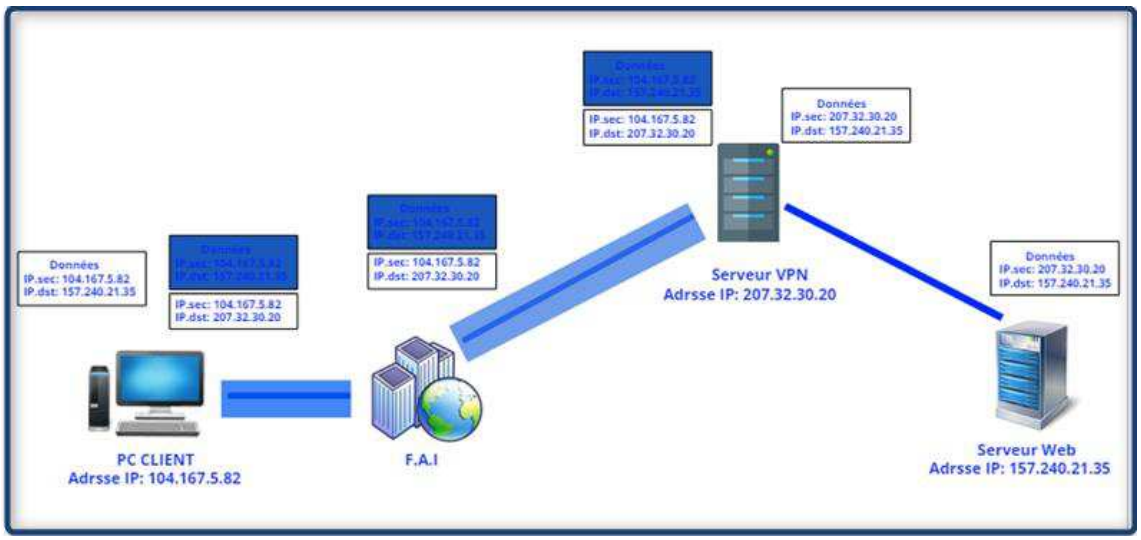

Figure 2. 8: Fonctionnement d'un VPN internet.

d) VPN en pratique :

Il y a plusieurs entreprises qui propose le service VPN web, et dans le choix d'un VPN on prendre en compte plusieurs facteurs comme la vitesse et la sécurité et la fiabilité plus le coûte et pour les services gratuits le nom et la popularité de l'entreprise, c'est un facteur essentiel. ExpressVPN et NordVPN sont des exemples d'un service VPN payant et TunnelBear, CyberGhost offrent un service gratuit.

Il y a deux méthodes d'accéder à un service VPN, la première ne nécessite pas l'installation d'un logiciel client juste d'ajouter une extension au navigateur web. Cette méthode permet juste de véhiculer le protocole HTTP/ HTTPs.

Figure 2. 9: L'extension VPN (de TunnelBear VPN).

Dans la deuxième méthode, l'installation d'un logiciel « agent » fourni par le fournisseur de service VPN est nécessaire, afin d'établir un tunnel vers un serveur VPN cette méthode et contrairement au premier permet de véhiculer différents protocoles de communication tels que SSH, SMTP, IMAP plus HTTP/HTTPs.

Figure 2. 10: l'application VPN (de TunnelBear VPN).

2.5.4 Réseau Tor:

a) Définition :

Tor « The Onion Routeur » est un réseau mondial et l'un des plus grands réseaux d'anonymat déployés, composé de milliers de relais (appelés nœuds) gérés par des bénévoles et de millions d'utilisateurs. Les utilisateurs de Tor utilisent ce réseau pour naviguer sur internet via une série de tunnels virtuels plutôt qu'en établissant une connexion directe, ce qui permet aux organisations et aux particuliers de partager des informations sur les réseaux publics sans compromettre leur vie privée [17].

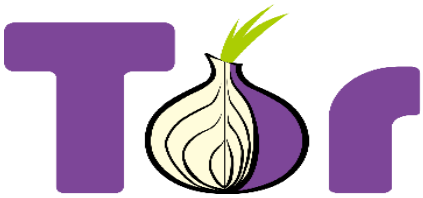

Figure 2. 11:Logo de réseau Tor.

Le projet Tor met à disposition des applications gratuites « prêtes à l'emploi » : le navigateur internet ''Tor Browser'' un système de messagerie instantanée ''Tor Messanger Beta'' ou encore une connexion ''Secure Shell'' (SSH), dans notre travail on s'intéresse à ''Tor Browser''.

b) Les relais Tor :

Le réseau Tor repose sur des relais ou nœuds mis en place par de nombreux bénévoles un peu partout dans le monde [figure 2.12] qui offre des machines capables de relayer le trafic des autres utilisateurs. N'importe quelle personne dans le monde peut participer au développement du réseau Tor en installant un proxy Tor sur leur machine, le programme et le manuel d'installation et de configuration sont fournis par le Projet Tor sur leur site officiel.

Figure 2. 12:La distribution de relais Tor dans monde.

Dans le réseau Tor, on trouve trois types de relais [18] :

Les relais d'entrée et relais intermédiaires : le relais d'entrée est le premier relais dans la chaîne des 3 relais construisant un circuit de Tor et le relais intermédiaire agit comme un saut entre les deux autres relais.

Le relais de sortie : est le dernier relais dans un circuit de Tor, celui qui envoie le trafic à sa destination. Les services auxquels les clients Tor se connectent (site Web) verront l'adresse IP du relais de sortie au lieu de leur adresse IP réelle (l'utilisateur Tor). Dans le cas d'une utilisation réseau Tor pour des activités illégales ce relais est exposé aux problèmes judiciaires, donc n'est pas recommander de l'installer à domicile et en général sont installé dans certaines institutions comme une université, une organisation liée à la vie privée ou quelques serveurs dédiés loués, qui sont mieux placés pour traiter ces problèmes.

Le Pont ou bridge : Le Pont ou bridge : Les bridges sont des relais d'entrée discrets utilisés lorsque l'accès habituel au réseau Tor est bloqué par le fournisseur d'accès, parce que la conception du réseau Tor signifie que les adresses IP des relais Tor sont publiques. Cependant, l'une des façons dont Tor peut être bloqué par les gouvernements ou les FAI est de mettre sur leur liste noire les adresses IP publiques de ces nœuds Tor. Les ponts Tor sont des nœuds du réseau qui ne sont pas répertoriés dans la liste publique des adresses de nœuds de réseau Tor, ce qui rend plus difficile le blocage des FAI et des gouvernements. Navigateur Tor doit être configuré pour utiliser un Pont. Le nombre de relais est variable d'une période à l'autre parce qu'il dépend de nombre de bénévoles. La [figure 2. 13] montre le nombre de relais et bridges de réseau Tor de début de l'année 2018 jusqu'à 20-05-2018.

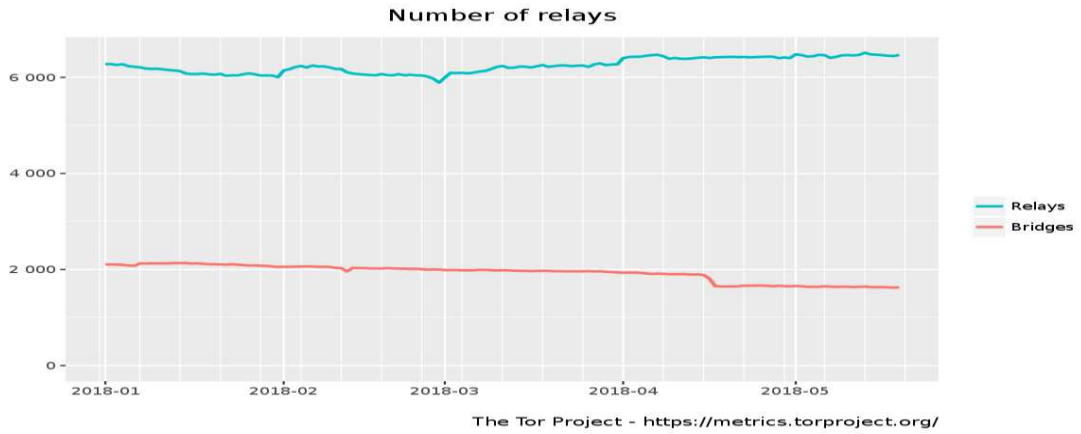

Figure 2. 13: Nombre de nœuds entre 01-01-2018 et 20-05-2018.

c) Serveurs d'annuaires :

Tor utilise les serveurs d'annuaire pour suivre les changements dans la topologie du réseau et l'état des nœuds. Chacun de ces serveurs d'annuaire agit comme un serveur HTTP, afin que les clients peuvent récupérer l'état du réseau actuel et une liste signée de tous les relais connus et dans cette liste se trouvent les certificats ´émis par les routeurs spécifiant leur clé, leur localisation et leurs politiques de sortie, et ainsi d'autres (OR) peuvent récupérer des informations d'État de réseau [15].

Les routeurs d'oignons publient périodiquement des déclarations signées de leur état à chaque serveur d'annuaire. Les serveurs d'annuaire combinent ces informations avec leurs propres vues de la vie du réseau, et génèrent une description signée (un répertoire) de l'état du réseau entier. Le logiciel client est pré-chargé avec une liste des serveurs d'annuaire et de leurs clés, pour qu'il puisse le connecter.

d) Routage :

Pour bénéficier du réseau Tor et pour devenir anonyme, le client « Onion Proxy (OP) » qui utilise le navigateur Tor, lorsqu'il lance le navigateur, l'application récupère une liste de nœuds à partir d'un serveur d'annuaire, chacun des nœuds connaît uniquement le nœud précédent et le nœud suivant. Ce dernier n'est alors pas en mesure de connaître le chemin complet.

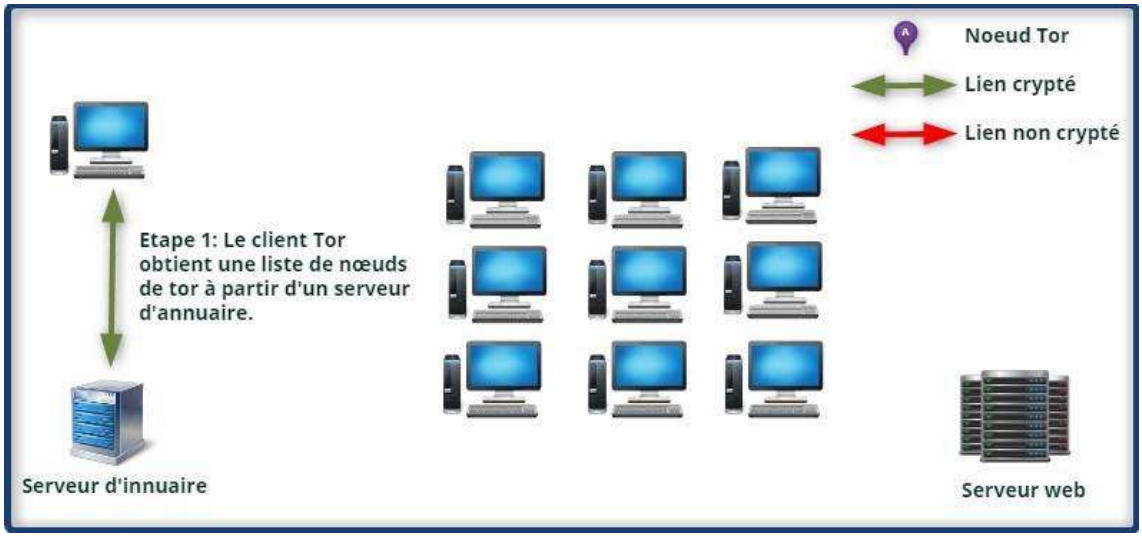

Figure 2. 14:Etapes 1 de routage dans le réseau Tor.

En suite l'application le client Tor choisit parmi les nombreux relais Tor, un chemin aléatoire composé de trois nœuds avant d'arriver au serveur destination. Le client Tor établit alors un circuit international. Le paquet sera routé à travers trois relais, ce qui rendra la source de la connexion difficilement identifiable, chacun des nœuds connaît uniquement le nœud précédent et le nœud suivant. Ce dernier n'est alors pas en mesure de connaître le chemin complet.

L'application utilise un seul nœud d'entrée tout au long d'une session de navigation, mais les deux autres nœuds varient par rapport au changement de serveur de destination.

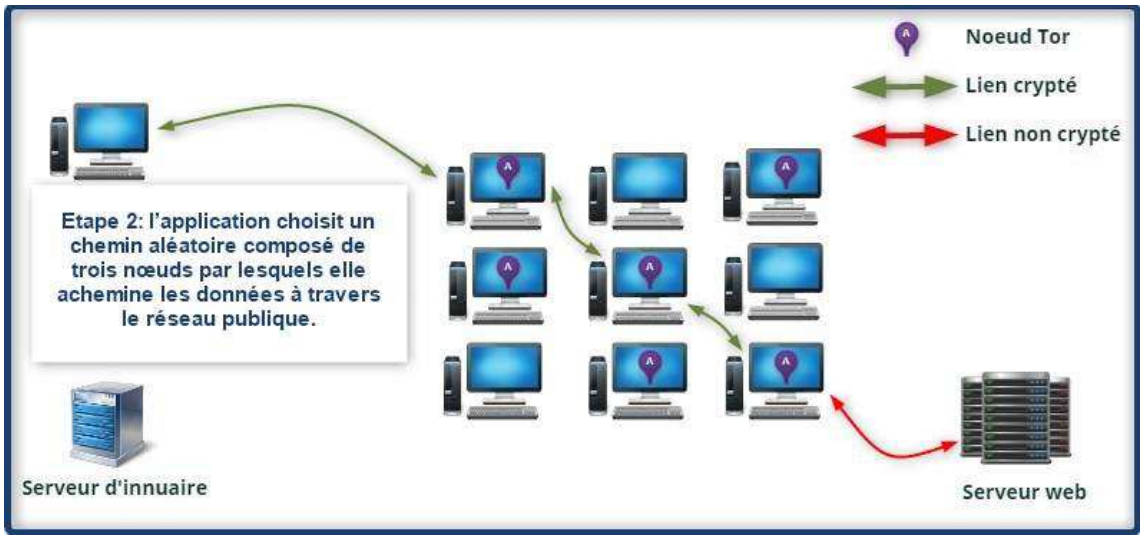

Figure 2. 15:Etapes 2 de routage dans le réseau Tor.

e) Le chiffrement

Toutes les connexions entre les nœuds ainsi qu'entre le client et le nœud d'entrée utilisent le protocole TLS. Avant que le paquet ne soit envoyé, en un premier temps et lors de l'établissement d'une session sécurisée, le client Tor et le nœud d'entrée « OR1 » négocient une suite de chiffrement et s'identifie en fin que chaque côté génère la clé symétrique numéro "1" ou la clé session "1" (les éléments de SLL Handshake).

Pour continuer dans le réseau, le client envoie une requête qui contient l'adresse de deuxième nœud « OR2 » à « OR1 » afin de lui demander d'étendre le réseau, en suite le client et « OR2» commencent les négociations de SLL Handshake à travers « OR1 » avant la génération de la clé symétrique numéro "2", le client peut maintenant aussi communiquer avec « OR2 » d'un maniéré sécurisée. Le client refait ces étapes avec nœuds de sotie « OR3 » pour que ces deux derniers génèrent la clé symétrique numéro "3" et avoir une liaison sécurisée [19].

Le client utilise ces "3" clés symétrique pour avoir un chiffrement successif par couche donc trois couches chiffrées encapsulent les données initiales comme un oignon, d'où le nom de "routage en oignon", et le chiffrage se fait de la manière suivante :

Le paquet est chiffré avec la clé « n » du dernier relais, le paquet obtenu est chiffré avec la clé du relais « n-1 » et ainsi de suite. Le chiffrement mis en place rend les données initiales inaccessibles pour toute personne située entre le client et le premier nœud de Tor, et cette

succession de couches évite ainsi qu'un des nœuds du circuit ne déchiffre le paquet dans son intégralité et soit en mesure de lire juste les données de routage qu'il concerne.

Pour cette partie, Tor utilise l'algorithme « Diffie-Hellman » pour l'échange de clés et le chiffrement RSA pour le cryptage asymétrique de secret pré-maître. La confidentialité des données échangées est obtenue grâce à un chiffrement de clés symétriques. Dans le réseau Tor, l'algorithme utilisé est l' « Advanced Encryption Standard » (AES). Tor utilise « Secure Hash Algorithm » (SHA) comme fonction de hachage pour vérifier l'intégrité des données.

f) Tor et la sécurité :

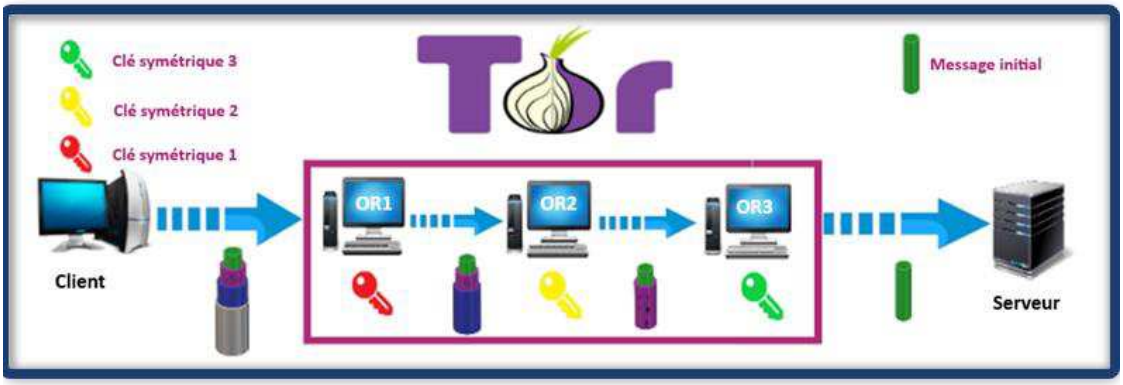

Figure 2. 16: Méthode de chiffrement Tor.

Tor sans doute le meilleur système permettant l'anonymat avec son routage en oignon et le chiffrement successif par couche, mais Tor n'assure pas la confidentialité absolue des échanges et les développeurs du réseau Tor le soulignent bien dans leur documentation [20] :

'' Tor anonymise l'origine de votre trafic et chiffre tout à l'intérieur du réseau Tor, mais il ne peut pas chiffrer votre trafic entre le réseau Tor et sa destination finale. Si vous envoyez des informations sensibles, vous devriez employer autant de précautions que lorsque vous êtes sur Internet. Utilisez HTTPS ou un chiffrement final similaire et des mécanismes d'authentification. ''

Comme on a déjà vu, le dernier nœud Tor déchiffre la dernière couche du paquet et envoie les données en clair à la destination finale. C'est à cet endroit ou certaines attaques peuvent être menées : en effet, pour quelqu'un qui se mit dans cet endroit pourra écouter ("sniffer") les paquets et récupérer des informations. C'est pourquoi il est recommandé d'utiliser le réseau TOR avec des flux chiffrés (HTTPS/SSL).

Le nœud de sortie est le seul maillon de la chaîne à avoir toutes les cartes en main pour lire les données des clients et il peut même injecter des logiciels malveillants ou des scripts dans le trafic destiné vers le client.

g) Utilisation de Tor dans une entreprise :

S'il est vrai que Tor peut être utilisé avec l'objectif légitime de l'anonymat sur Internet, il peut aussi représenter un problème gigantesque pour une entreprise, afin de faciliter la compréhension on doit décomposer ces risques en deux parties selon la direction de trafic :

1. Les risques liés au trafic sortent :

Le réseau Tor crypte tout le trafic sur le réseau et rend très difficile la surveillance des activités. Les employés peuvent utiliser réseau Tor pour:

- Contourner les politiques de sécurité et les contrôles de l'organisation très facilement.

- Accéder au web profond (deep web) : les employés peuvent utiliser Tor pour accéder au web profond et utilisent les ressources de l'entreprise pour des activités malveillantes ou criminelles ce qui expose l'entreprise à des problèmes judiciaires et donne une mauvaise image de l'ensemble de l'entreprise. En ajoutant à cela, que le web profond renferme de tous genres de logiciels malveillants et virus qui pouvant créer des risques de sécurité.

- Exploiter des Bitcoins : les employés peuvent utiliser les réseaux et les ressources de l'entreprise pour exploiter des Bitcoins.

- Contrôler les Botnets et les logiciels malveillants : les employés peuvent utiliser Tor comme un canal de communication afin de contrôler à distance les ordinateurs piratés (botnets), et les logiciels malveillants comme cheval de Troie ou Ransomware.

- le propriétaire de nœud de sortie peut surveiller le trafic transitant par son appareil et capturer toute information non cryptée telle que le nom d'utilisateur, mot de passe.

2. Les risques liés au trafic entrant :

Ces risques sont liés principalement aux nœuds du sortie de réseau Tor et qui sont les suivants:

- Attaques de logiciels malveillants et de botnets : les utilisateurs d'un des "nœuds de sortie" peuvent ajouter un logiciel malveillant ou un script au trafic, et à tout téléchargement effectué

à partir de réseau Tor, ce qui expose le réseau de l'organisation à une infection par logiciel malveillant.

- Attaques DDoS : le trafic réseau Tor peut provoquer une utilisation élevée de la bande passante du réseau d'entreprise, ce qui expose l'organisation de manière permanente à une attaque DDoS.

h) Le blocage de réseaux Tor dans une entreprise :

Le blocage de réseau Tor dans un d'entreprises est très compliqué, cependant les entreprises peuvent appliquer des mesures d'atténuation qui permettent de limiter l'utilisation de réseau Tor [21]:

- Règlement sur l'utilisation de Tor : le règlement de sécurité de l'entreprise doit interdire impérativement l'utilisation de l'ensemble de réseau Tor sur les ressources de l'entreprise. Parallèlement, il est important d'informer l'ensemble des employés de l'entreprise que l'utilisation de Tor sur le réseau de l'entreprise est strictement interdite et considérée comme une violation majeure de règlement de sécurité. Cette politique doit être soutenue par des pénalités sévères pour avoir exécuté des applications non approuvées.

- La sensibilisation et la formation : tous les employés doivent être conscients des risques liés à l'utilisation du Tor dans leur réseau d'entreprises.

- Sur le côté technique, le filtrage des adresses IP correspondantes aux nœuds Tor (sont disponibles publiquement) peut limiter l'utilisation de réseau Tor.

Une autre solution pour bloquer le réseau Tor dans les entreprises consiste à bloquer via un pare-feu les ports fréquemment utilisés par Tor. Aussi d'autres solutions seront proposées dans le chapitre suivant.

Conclusion :

L’internet d’aujourd’hui interpelle les gens à protéger leur vie privée en ligne, et l’anonymat et le chiffrement sont des moyens pour protéger celle-ci et de préserver la liberté d'expression sur Internet.

Cependant il y a plusieurs méthodes pour être anonyme sur le net, comme l’utilisation d’un Proxy, VPN, ou le réseau Tor. Tor sans doute, est le meilleur système permettant l’anonymat avec son routage en oignon et le chiffrement successif par couche, cette solution présente également des limites. L’utilisation de cet outil à partir d'un réseau d'entreprise peut exposer l’entreprise à divers risques de sécurité.

Le blocage de réseau Tor dans un réseau d’entreprise est très compliqué, cependant il y a des solutions possibles pour minimiser l’utilisation du réseau d’anonymisation, comme le filtrage des adresses des nœuds ou le blocage des Ports utiliser par Tor et d’autres solutions qu’on va les proposer dans le troisième chapitre.

Chapitre3: Extraction des empreintes du réseau Tor

3.1 Introduction :

Le réseau d'anonymat Tor est un outil libre et important qui permet aux millions de personnes de protéger leur vie privée en ligne, mais il reste imparfait. L'utilisation de cet outil à partir d'un réseau d'entreprise peut exposer l'entreprise à divers risques de sécurité et à des problèmes judiciaires. En effet, les organisations et entreprises doivent commencer à prêter attention au risque de l'utilisation du réseau Tor dans leurs réseaux.

La détection de Tor dans un réseau d'entreprise est très compliquée et nécessite des mises à jours permanente des règles de sécurité (adresses IP, empreintes, etc.). Les organisations et entreprises devraient envisager le déploiement de plusieurs solutions, pour augmenter les chances d'empêcher l'utilisation de Tor dans leur réseau.

La détection de Tor nécessite une analyse du trafic web provenant du réseau Tor et du trafic web normal, et faire une comparaison entre les deux. Les différences entre les deux trafics et le relèvement d'une empreinte digitale permettent d'identifier le réseau Tor.

Dans ce chapitre on présente les différentes méthodes utilisées pour la détection de l'utilisation du réseau Tor dans notre réseau et pour cela on a décidé de répartir notre travail en trois sections réparti comme suit :

- La première section présente la méthodologie de recherche.

- La seconde section porte sur l'analyse en détail du trafic provenant du navigateur Tor et d'autres navigateurs, afin de relever des différences qui permettent de distinguer l'utilisation du réseau Tor.

- Et enfin la troisième section porte sur l'utilisation des résultats de deux premières sections pour extraire une empreinte digitale qui identifie le réseau Tor, afin de l'implémenter dans un système de détection d'intrusion (Snort) pour détecter l'utilisation du réseau Tor.

3.2 La méthodologie de recherche :

À travers notre recherche, nous allons essayer de décrire comment Tor révèle sa présence en soulignant les différences du trafic Tor par rapport au trafic web normal. Cela nous oblige à décrire aussi le trafic web normal. En raison de cette différence on peut proposer plusieurs solutions pour la détection du réseau Tor. Et cela afin de cerner notre problématique et d'apporter des éléments de réponses à un certain nombre de questions posées au début de ce travail.

3.2.1 Les démarches suivies dans notre recherche :

Pour répondre à notre problématique, nous avons utilisé les méthodes et techniques suivantes :

- **La technique documentaire :** qui nous a permis de définir les concepts théoriques sur le sujet de notre recherche.
- **Capture des données :** qui nous a permis de capturer le flux de données provenant du différents navigateurs.
- **Méthode d'analyse des données :** qui nous a permis de relever des différences qui permettent de distinguer l'utilisation du navigateur Tor.
- **Méthode pratique :** qui nous a permis d'implémenter ces différences dans un Système de détection d'intrusion réseau (NIDS) Snort, afin de valider nos solutions et tester leur fiabilité.

3.2.2 Matériel et logiciel utiliser dans notre recherche :

Nous avons mené notre recherche dans un environnement ouvert. Un réseau local au domicile connecté à internet, et les expériences ont été faites sur:

- Un ordinateur portable Dell avec un processeur Intel core i5-3337u a 1.80 GHz et de 6 Go de la RAM.
- Un ordinateur bureau avec un processeur Intel Core 2 Duo 2.93GHz et de 3 Go de la RAM.
- Le système d'exploitation Windows 10 64bit.
- Linux Ubuntu 18.04 64 bit.
- VMware Workstation 12.0 virtual machine avec Ubuntu 16.04.3 64 bit.

Tout au long de notre recherche on utilise les logiciels suivants :

- Wireshark version 2.6.1 64 bit.
- COMODO Firewall version 10.2.0.6526 64 bit.
- Une plate-forme de développement Web WampServer version 3.1.0 64 bit.
- Les navigateurs web : Tor browser de version 7.5 à 7.5.4, Mozilla Firefox de version 42.0.01 jusqu'à 60.0.1, Google Chrome de 1.3.33.7 jusqu'à 60.0.3359.181. Nous avons utilisé plusieurs versions pour augmenter la précession de notre recherche.

3.2.3 Objectif de notre recherche :

L'objectif de notre recherche est de crée des règles Snort pour détecter l'utilisation du réseau Tor dans une entreprise.

3.3 L'analyse du trafic web de différant navigateur :

3.3.1 Capteur des données :

Pour capturer le trafic, on a utilisé Wireshark sous Windows 10 :

Wireshark est un logiciel d'analyse réseau (sniffer) qui permettant de visualiser l'ensemble des données transitant sur la machine qui l'exécute, et d'obtenir des informations sur les protocoles applicatifs utilisés. Les octets sont capturés en utilisant la librairie réseau PCAP, puis regroupés en blocs d'informations et analysés par le logiciel [22].

Pour capturer le trafic avec Wireshark, et une fois que l'application est exécuté, on lance la capture de trame à travers l'ongle « démarrage la capture de paquet ».

Ensuite, nous avons lancé le navigateur web et saisi des adresses web (URL), une fois les pages complétements chargées, nous avons arrêté la capture et sauvegardé le fichier de capture.

La figure 3.1 montre la fenêtre de Wireshark après la capture des paquets et on peut la décomposer on trois zone :

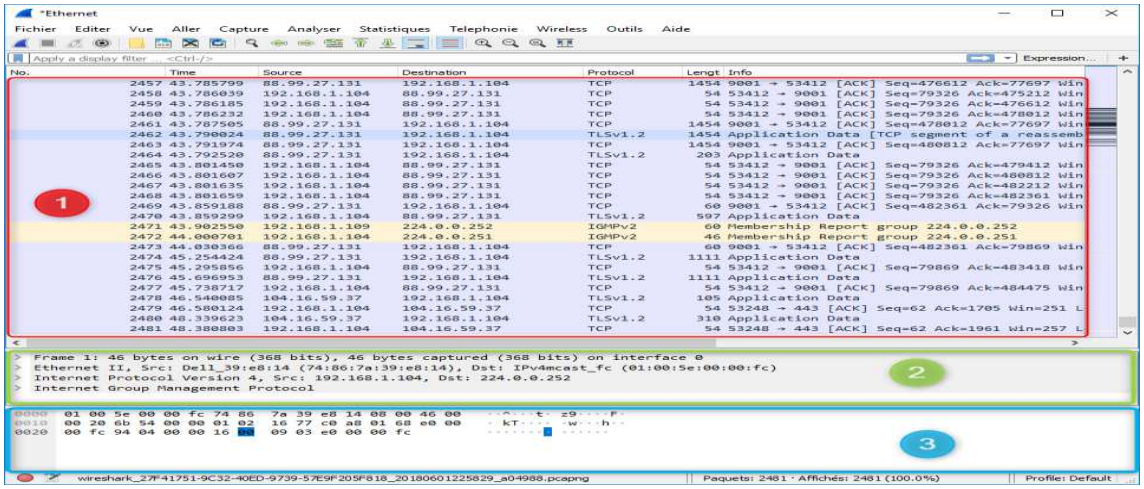

Figure 3. 1: Fenêtre de Wireshark après le capture.

- Zone numérotée (1) sur la figure 3.1 : liste de l'ensemble des paquets capturé.
- Zone numérotée (2) sur la figure 3.1 : affiche le détail d'un paquet sélectionné.
- Zone numérotée (3) sur la figure 3.1 : présente l'ensemble du paquet sous forme octale et ASCII.

La capture du trafic a été effectuée sur plusieurs reprises entre la période 14-2-2018 et 01-06-2018, nous avons capturé les paquets de chaque navigateur séparément des autres pour augmenter la fiabilité de notre recherche avec un total de 40 captures.

3.3.2 Les démarches utilisées pour notre analyse :

Réseau Tor utilise le protocole TLS qui établit une session chiffrée entre le client Tor et le nœud d'entrée du réseau Tor. TLS nécessite un transport fiable donc il est basé sur le protocole TCP. D'abord le client Tor établit une connexion TCP avec le nœud d'entrée, ensuite, il établit une session TLS qui commence toujours par l'échange des messages de négociation SSL (SSL Handshak). Après l'établissement de connexion TLS, les données échangées entre le client Tor et le nœud d'entrée seront chiffrées et impossibles à analyser.

Au cours de ce chapitre, nous utilisons « Wireshark » pour examiner les paquets de connexion TCP et les messages de négociation SSL des différents navigateurs. Nous présentons le contexte de notre recherche en le décomposant en trois parties:

- L'étude des étapes d'établissement de connexion entre le client Tor et nœud d'entrée du réseau Tor.
- Analyse et comparaison des paquets TCP de l'établissement de connexion en trois étapes (TCP three ways handshake) du trois navigateurs.
- Analyse et comparaison des paquets TLS de protocole « SSL handshake » de trois navigateurs.

3.3.3 Etude des étapes d'établissement de connexion entre navigateur Tor et nœud d'entrée du réseau Tor :

Pour étudier les étapes d'établissement de connexion entre navigateur Tor et nœud d'entrée. Nous avons utilisé COMODO FIREWALL et le site web https://metrics.torproject.org fournit par les développeurs du réseau Tor, en passent par les étapes suivantes :

a) Lancement du navigateur Tor :

Figure 3. 2: Navigateur Tor phase d'établissement d'une connexion.

Au même temps, nous avons visualisé les connexions établées par le navigateur Tor sur KOMODO FIREWALL :

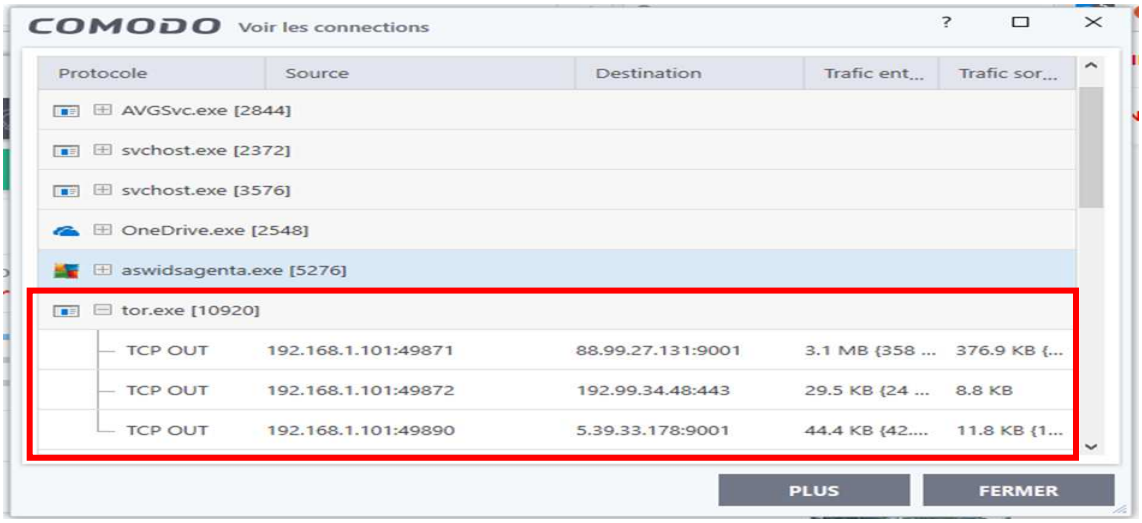

Figure 3. 3: Les connexions établées par navigateur Tor.

On remarque dans la [figure 3.3], que le navigateur Tor a établie 3 connexion vers trois adresses différentes.

« 88.99.27.131 :9001 », « 192.99.34.48 :433 », « 5.39.33.178 :9001 ».

Nous avons accédé au site web « torproject.org » à partir du navigateur Tor et l'application a choisi un chemin aléatoire composé de 3 nœuds.

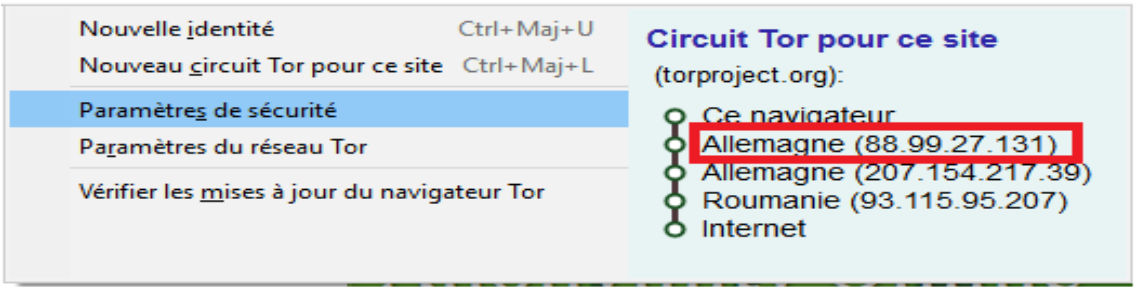

Figure 3. 4: Circuit Tor vers le site torproject.org.

On remarque que l'un des adresses capturer par KOMODO FIREWALL est l'adresse de nœud d'entrée (88.99.27.131).

Les autres adresses sont ceux des ''serveurs d'annuaires '', contacter par le navigateur Tor au lancement de l'application pour récupérer les listes des nœuds.

Les développeurs de Tor mettent à la disposition de leur utilisateur un outil de recherche des nœuds qui affiche des informations sur chaque nœud et leur position dans le réseau Tor. Il fournit aussi des informations utiles sur la façon dont les relais sont configurés et ces fonctionnalités. L'outil est accessible via le site : https://metrics.torproject.org/rs.html#search.

1) Nous avons utilisé l'outil de recherche Tor pour vérifier, si les deux adresses capturées par « KOMODO FIREWARE » sont des adresses des serveurs d'annuaire du réseau Tor.
   - L'adresse : "5.39.33.178 :9001" et "192.99.34.48 :433".

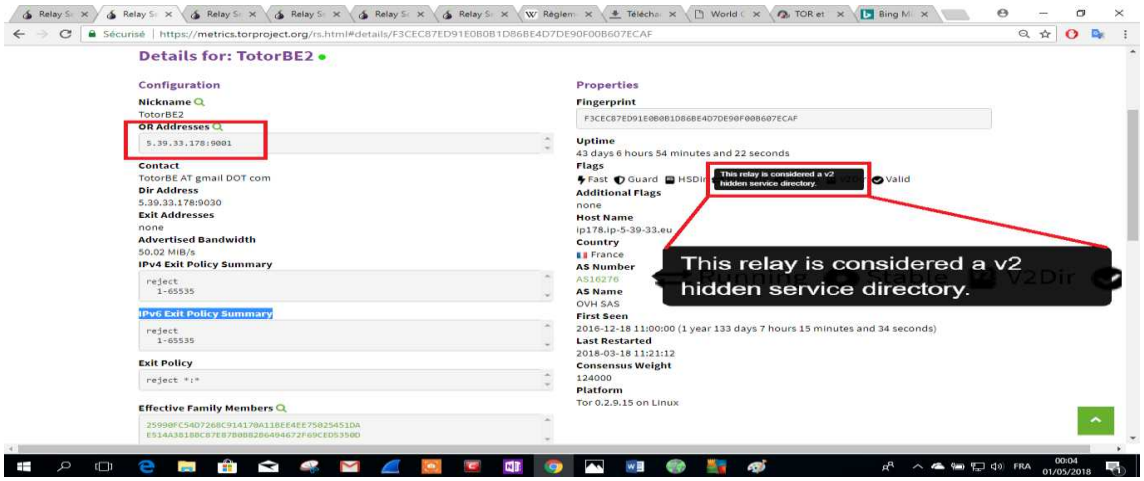

Figure 3. 5: L'outil de recherche Tor.

Nous avons trouvé que ces deux nœuds pouvant fonctionner comme des serveurs d'annuaire caché. Les résultats expérimentaux confirment l'étude théorique d'écrit dans le chapitre deux.

3.3.4 Les paquets TCP de l'établissement de connexion en trois étapes :

Selon le protocole de communication TCP, une connexion entre un client et un serveur s'établit en trois étapes : c'est le « **three-way handshake** ».

Dans cette partie, nous allons analyser les paquets TCP (SYN, SYN-ACK, ACK) résultant de l'établissement de connexion en trois étapes entre :

- Navigateur Tor et le serveur d'annuaire, son adresse IP « 88.99.27.131 ».
- Navigateur Tor et le nœud d'entrée Tor, son adresse IP « 213.32.95.53 ».
- Navigateur Mozilla Firefox et le site web « 3wshcooles.com », son adresse IP « 192.299.133.221 ».
- Navigateur Google chrome et ce dernier site web.

Ensuite, nous allons comparer les résultats d'analyse des paquets du navigateur Tor avec les résultats d'analyse des deux autres navigateurs, afin de relever les différences qui vont permettre de distinguer l'utilisation du réseau Tor.

Nous avons commencé notre analyse par le paquet SYN [le paquet 57 dans la figure 3.6] qui corresponde au premier paquet TCP, dans la procédure d'établissement de connexion en trois étapes entre navigateur Tor et le serveur d'annuaire Tor :

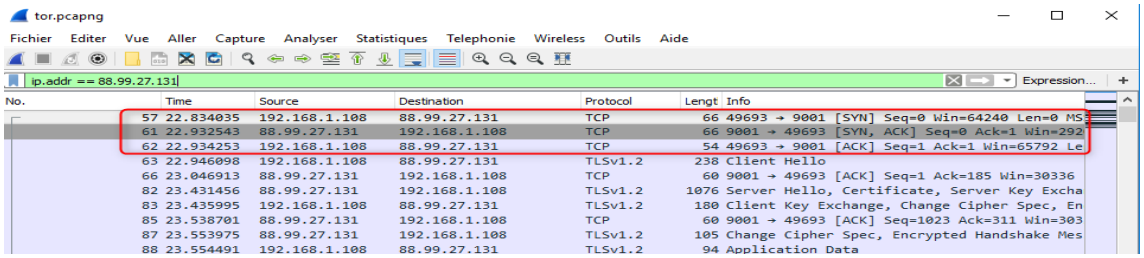

Figure 3. 6: Les paquets capturer.

Nous avons sélectionné le paquet 57, et lorsqu'un paquet est sélectionné, la zone centrale de « Wireshark » permet de visualiser clairement les différentes couches d'encapsulation du paquet [Figure 3.7] :

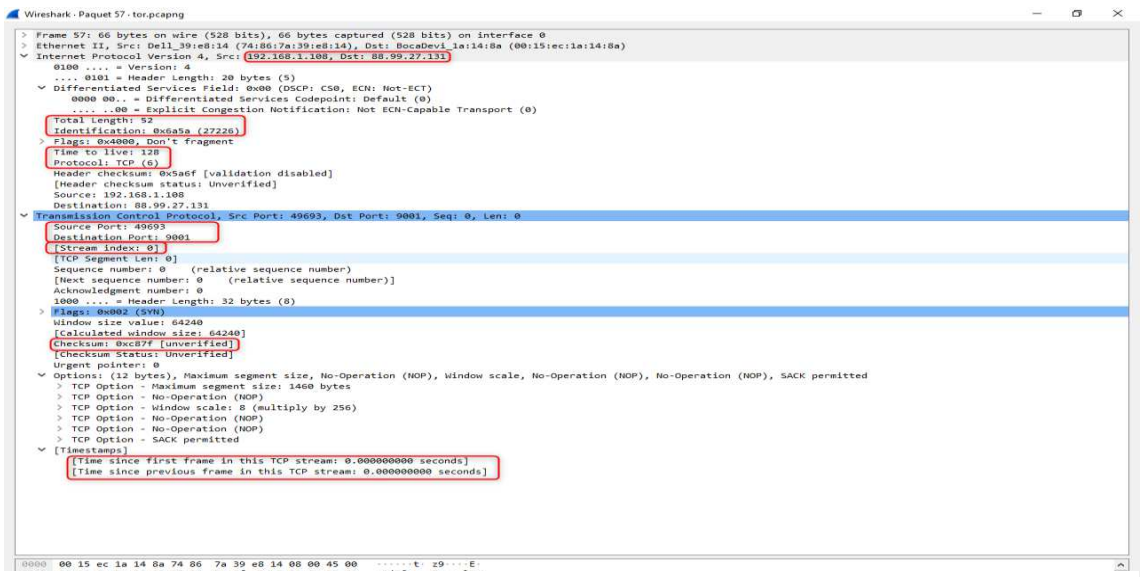

Figure 3.7 : Premier paquet TCP de l'établissement de connexion en trois étapes

À partir de ces différentes couches, on peut extraire les informations suivantes :

- Les adresses IP source et destination, numéro de porte source et destination, le type d'adressage et le protocole utiliser.

- Indentification : chaque connexion doit être identifiée de manière unique. Ceci est fait en utilisant la paire d'identifiants de socket (combinaison d'adresse IP et Port) correspondant aux deux extrémités de la connexion.
- MSS (Maximum Segment Size). Elle sert à déterminer la taille maximale du segment que le module TCP accepte de recevoir. Au moment de l'établissement d'une connexion, le module émetteur annonce sa taille de MSS [7].
- Les numéros de séquence : sont utilisés pour décompter les données dans le flux d'octets, le numéro de séquence indique le premier octet des données. Durant cet échange initial, les numéros de séquence des deux parties sont synchronisés.
- TTL (Time To live) : indique le temps pendant lequel une information doit être conservée [1].
- Stream index : Stream index ou l'index de flux est un mappage Wireshark interne.
- Windows size value : est une annonce de la quantité de données (en octets) que le dispositif récepteur est prêt à recevoir à tout moment. Le périphérique de réception peut utiliser cette valeur pour contrôler le flux de données ou comme mécanisme de contrôle de flux [1].
- RTT to ACK : Round Time Trip to acknowledgement. RTT to ACK est un mécanisme de temporisation et de retransmission. RTT est le temps que met un signal pour parcourir l'ensemble d'un circuit fermé. Dans les faits, le délai avant la retransmission, doit être supérieur à RTT moyen d'un segment.

D'abord, nous avons utilisé ces informations pour remplir un tableau, Ensuite nous avons fait les mêmes procédures avec les deux autres paquets SYN-ACK et ACK de cette connexion.

Nous avons fait les mêmes étapes avec les autres connexions. Les tableaux 3.1, 3.2 et 3.3 englobent toute l'analyse.

Le premier paquet TCP (SYN):

	Tor (avec 88.99.27.131)	Tor (avec 213.32.95.53)	Firefox	Google chrome
Type	IPv4 (0x0800)	IPv4 (0x0800)	IPv4 (0x0800)	IPv4 (0x0800)
Protocole	TCP (6)	TCP (6)	TCP (6)	TCP (6)
Port	49693	49694	50752	64911
Port	9001	433	433	433
MSS	1460	1460	1460	1460
La langueur total(IP)	52	52	52	52
Identification	0x6a5a (27226).	0x1f25 (7973)	0x29ce	0x8ce1
TTL	128	128	128	128
Numéro de séquence	0	0	0	0
Stream index	0	1	10	12
Flags	0x002(SYN)	0x002(SYN)	0x002 (SYN)	0x002(SYN)
Windows size value	64240	64240	64240	64240

Tableau 3.1: Le premier paquet TCP dans l'établissement de la connexion en trois étapes.

Le deuxième paquet TCP (SYN-ACK):

	Tor (avec 88.99.27.131)	Tor (avec 213.32.95.53)	Firefox	Google chrome
Type	IPv4 (0x0800)	IPv4 (0x0800)	IPv4 (0x0800)	IPv4 (0x0800)
Protocole	TCP (6)	TCP (6)	TCP (6)	TCP (6)
Port	9001	433	433	433
Port	49693	49694	50752	64911
MSS	1400	1400	1380	1400
La langueur total(IP)	52	52	40	52
Identification	0x0000 (0)	0x0000 (0)	0x0000 (0)	0x0000(0)
TTL	48	51	53	52
Numéro de séquence	0	0	0	0
Stream index	0	1	16	12
Flags	0x012 (SYN/ASK)	0x012(SYN/ASK)	0x012 (SYN/ASK)	0x012(SYN/ASK)
Windows size value	29200	29200	65535	65535
SEQ/ACK analyses				
RTT to ACK	0.098508000 seconde	0.08525000 s	0.08786500 S	0.22856300 s

Tableau 3.2 : Le deuxième paquet TCP dans l'établissement de la connexion en trois étapes

Le troisième paquet TCP (ACK):

	Tor (88.99.27.131)	Tor (avec 213.32.95.53)	Firefox	Google chrome
Type	IPv4 (0x0800)	IPv4 (0x0800)	IPv4 (0x0800)	IPv4 (0x0800)
Protocole	TCP (6)	TCP (6)	TCP (6)	TCP (6)
Port	49693	49694	50752	64911
Port	9001	433	433	433
MSS				
La langueur total(IP)	40	40	40	40
Identification	0x6a5b(27227)	0x1f26 (7974)	0x29cf	0x650d (25869)
TTL	128	128	128	128
Numéro de séquence	1	1	1	1
Stream index	0	1	10	12
Flags	0x010 (ASK)	0x010 (ASK)	0x010 (ASK)	0x010 (ASK)
Windows size value	257	257	257	257
SEQ/ACK analyses				
RTT to ACK	0.0017100 s	0.000543000 s	0.005643000 S	0.09466500 S

Tableau 3.3 : Le troisième paquet TCP dans l'établissement de la connexion en trois étapes.

Constatation :

Il y a une différence au niveau de :

- Les ports sources : c'est totalement logique parce qu'ils sont générés d'une manière dynamique par chaque application.
- Les Ports de destinations : les nœuds d'entrées Tor utilisent le port 9001 à la place du port 443 (le port par défaut de protocole SSl (HTTPS)).
- Identification : il y a une différence entre les quatre cas, mais cette différence est totalement normale, car chaque connexion doit être identifiée d'une manière unique.
- Stream index : on ne le prend pas en considération parce que est un mappage Wireshark interne, cela veut dire que c'est une valeur calculée et attribuée par Wireshark.
- RTT to ACK : ces caractères varièrent d'une connexion à l'autre.

Les résultats de cette analyse, nous permettent de constater qu'il n'y a pas une différence qui peut distinguer le réseau Tor dans les paquets TCP de l'établissement de la connexion en trois étapes.

Pour détecter l'utilisation du réseau Tor, on doit récupérer la liste des adresses IP des nœuds et les numéros des ports utilisés par ces derniers.

La liste des adresses des nœuds du réseau Tor peut être récupérée à partir de site web : https://www.dan.me.uk/tornodes. Ainsi que la librairie onion_py sous Linux permet la récupération de cette liste.

Récupération de liste des adresses des relais Tor en utilisant onion_py et un code python sous Linux :

OnionPy : est une société spécialisée dans l'analyse de données. Ils ont constaté l'importance de la collection des données de nos jours, et que la plus grande source de données au 21ème siècle est bien Internet. De ce fait, ils ont mis en place une infrastructure où ils collectent les données pour ensuite les traiter et les analyser. Dans cette infrastructure, ils ont une banque d'informations, des services d'analyse de données de la data-science, des applications, et plusieurs plate-formes qui les rendent accessibles aux utilisateurs et offrant de ce fait un service à la demande.

Parmi les services offerts, il y a celui à propos du réseau Tor, où une API « Onionoo » a été mise en place. Dans notre projet, on a utilisé cette API (application programming interface) à l'aide d'une bibliothèque python appelé aussi onion_py, pour scripter la récupération de la liste des adresses des nœuds Tor.

Pour cette étape, nous avons utilisé le système Ubuntu sur une machine virtuelle VMware :

- D'abord, nous avons installé le paquet « OnionPy » :

```
sudo pip install OnionPy
```

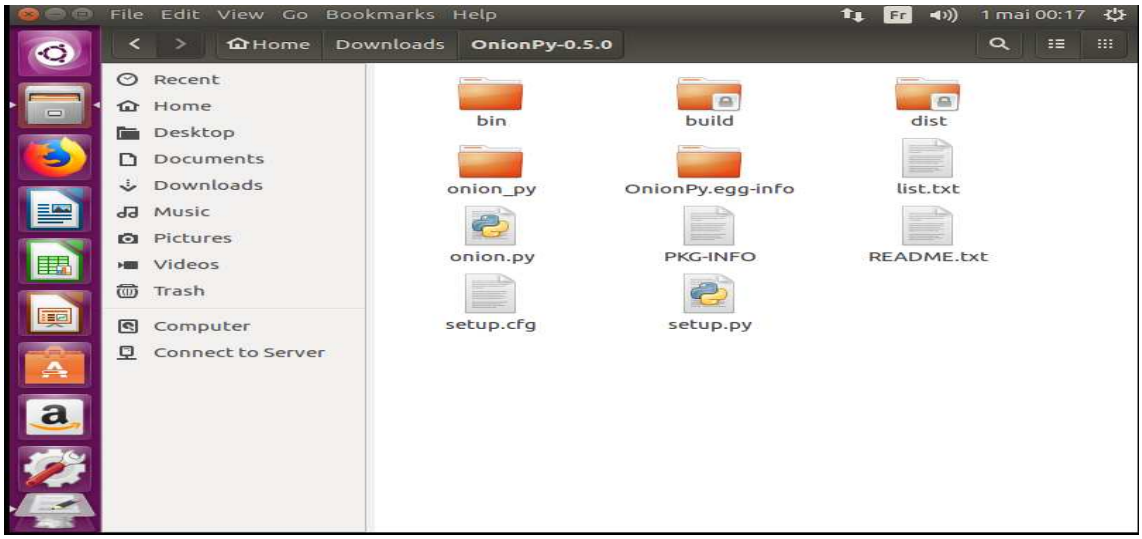

Figure 3. 8: Les fichiers de Onion_Py

- Ensuite, nous avons modifié dans les fichiers (manager.py et setup.py) pour rendre la bibliothèque OnionPy compatible avec la version actuelle de OnionOO (la version actuelle de OnionOO est 6.0)
- Et nous avons exécuté le code python suivant :

```
from onion_py.manager import Manager
from onion_py.caching import OnionSimpleCache
manager = Manager(OnionSimpleCache())
sd = manager.query('details')
len(sd.relays)
for relay in sd.relays:
 for addr in relay.or_addresses:
   print(addr)
```

source de code ‘’ https://github.com/duk3luk3/onion-py/.

nous avons ajouté la commande ‘’fh = open('list.txt', 'w')’’ et ‘’fh.write(addr + "\n")’’ au code pour enregistrer la liste dans fichiers .txt

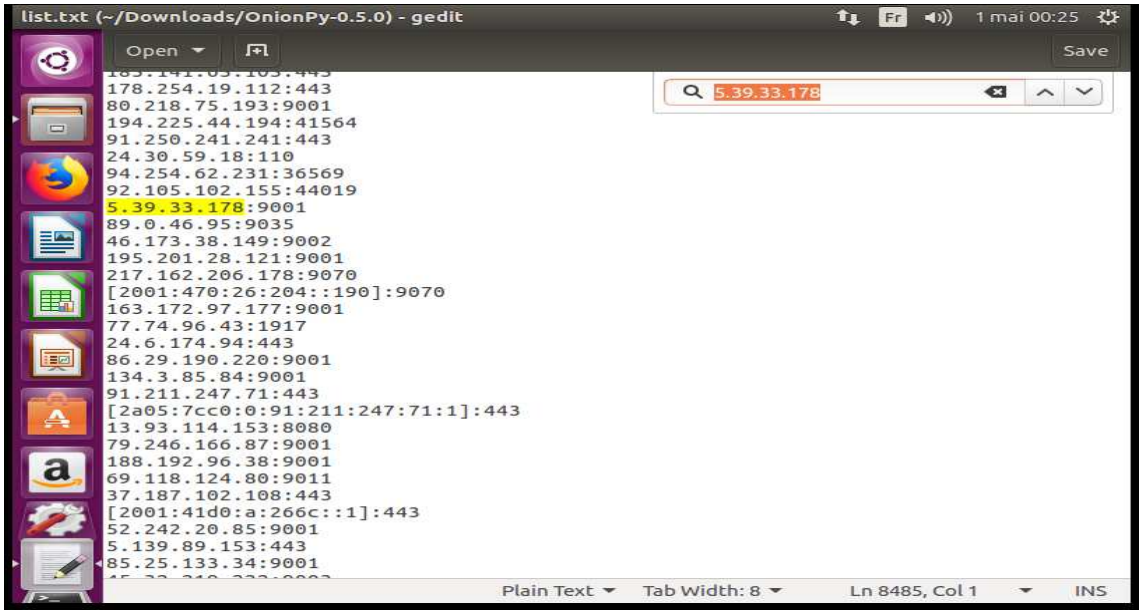

Figure 3. 9: Liste des nœuds Tor.

3.3.5 Les paquets TLS de protocole d’établissement de connexion SSL « SSL handshake » :

SSL handshake et comme nous avons décrié dans le chapitre deux, c’est un protocole de négociation, utiliser pour négocier des clés et des protocoles de chiffrement qui seront utilisé tout au long d’une session sécurisée. Dans cette partie, nous allons analyser et comparer les paquets d’établissement de connexion SSL entre « navigateur Tor et le premier nœud de circuit Tor » d’un côté et celle de Google chrome avec plusieurs serveurs web et Mozilla Firefox avec les mêmes serveurs.

Dans le tableau 3.4 nous avons mentionné les adresses des nœuds Tor et celle des serveurs web utilisés dans notre recherche :

Serveurs de destination	L'adresse IP
Nœud d'entrée Tor 1	88.99.27.131
Nœud d'entrée Tor 2	213.32.95.53
Nœud d'entrée Tor 3	5.39.33.178
www.wikipedia.org	91.198.174.192
www.microsoft.com	2.21.180.244
www.w3schools.com	192.229.133.221
www.netacad.com	23.223.95.225

Tableau 3.4 : Les adresses des noeuds d'entrées et des serveurs web.

Dans Wireshark nous avons utilisé le filtre « ip.addr == <adresse de serveur destination> and ssl.handshake » pour isoler les paquets de « ssl handshake » qui concerne l'adresse < serveurs destinations > des autres paquets :

La figure 3.10 montre les messages échangés lors de l'établissement d'une session sécurisée « ssl handshake ». Dans notre recherche, on s'intéresse seulement aux trois premiers messages « ''client Hello'', ''server Hello'', ''Certificate, Certificate Status, Server Hello Done''».

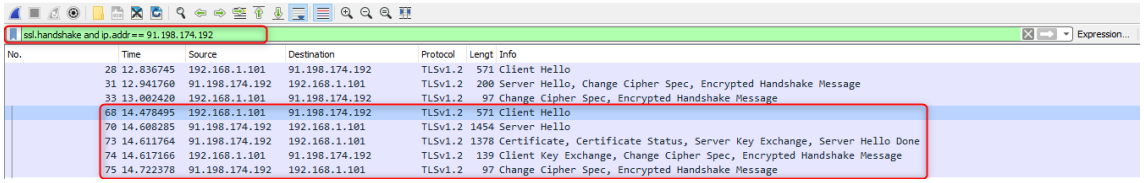

Figure 3.10: les paquets SSL handshake échanger entre Google chrome et wikipedia.com.

Navigateur Tor envoie les deux messages ''Server Hello'' et '' Certificate, Certificate Status, Server Hello Done'' dans un seul message.

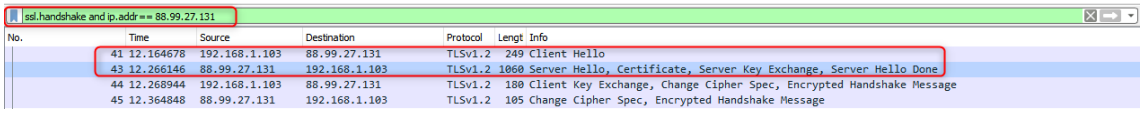

Figure 3.11: Les paquets SSL handshake échanger entre navigateur Tor et nœud d'entrée.

Après l'analyse des différentes captures, nous avons trouvé les résultats suivants :

a) Message Client Hello :

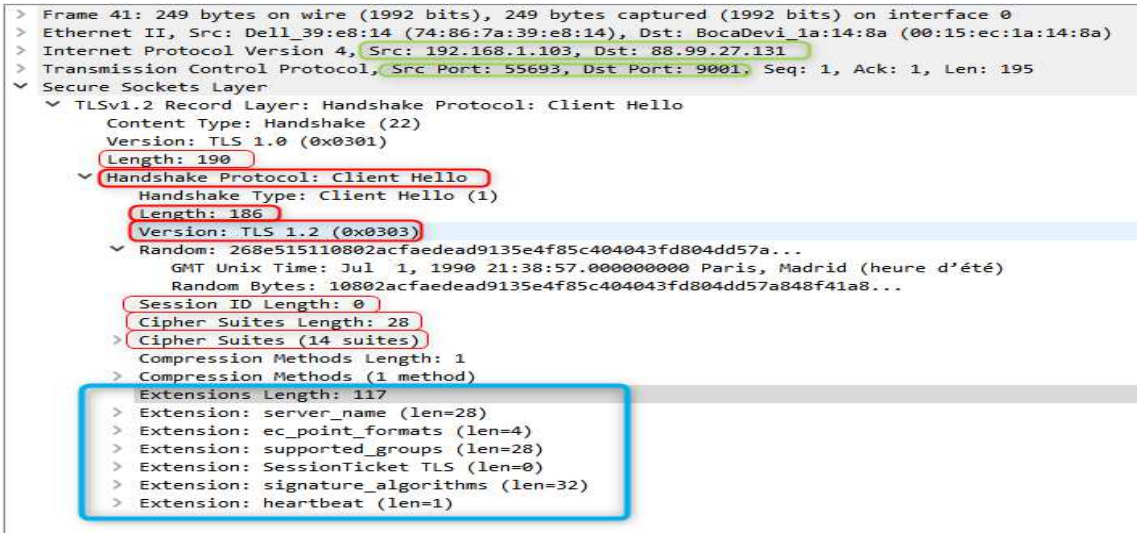

Figure 3. 12: Message Client Hello envoyer par navigateur Tor

La longueur totale « Length » de message Client Hello envoyé par Navigateur Tor est largement petite par rapport à la longueur de message envoyé par Google chrome ou Mozilla qui est fixé sur 512 octets, les deux navigateurs ajoutent une suite de zéro également appeler un ‘’padding’’ à la fin de message pour étendre cette valeur. La longueur du message envoyé par navigateur Tor est généralement entre 168 et 200 octets.

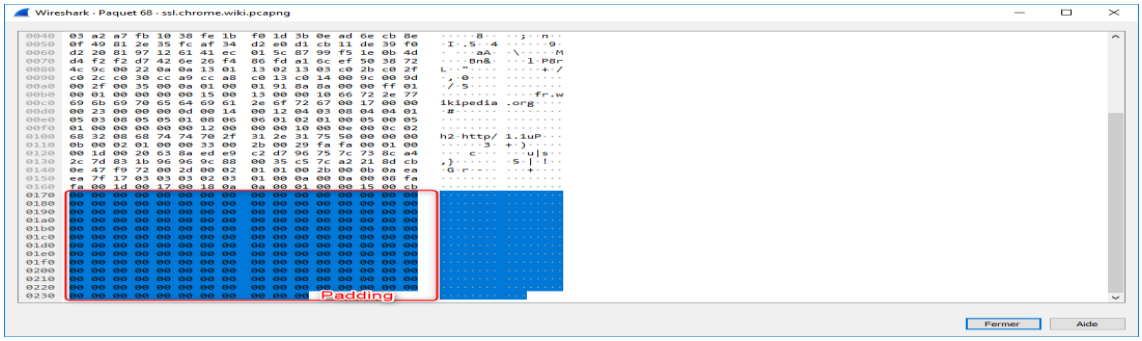

Figure 3. 13: Padding ajouter par les navigateurs Google chrome et Mozilla.

Dans l'ongle « Random » on trouve la date et l'heure d'initiations de message Client Hello, dans le message générer par navigateur Tor la date et l'heure sont totalement déréglées.

‘’ **Random ou la chaîne d'octets aléatoire :** est généré à partir de la date et l’heure d’ordinateur de client et qui sera utilisé avec la chaîne d’octets aléatoire envoyer par le serveur pour générer le « secret pré-maître » [25].

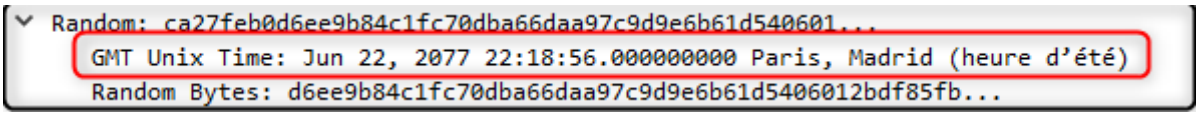

Figure 3. 14: L'ongle Random.

Navigateur Tor propose 14 suites de chiffrement dans un ordre bien précis. Même Mozilla Firefox propose 14 suites dans un ordre différent, Google chrome utilise 17 suites.

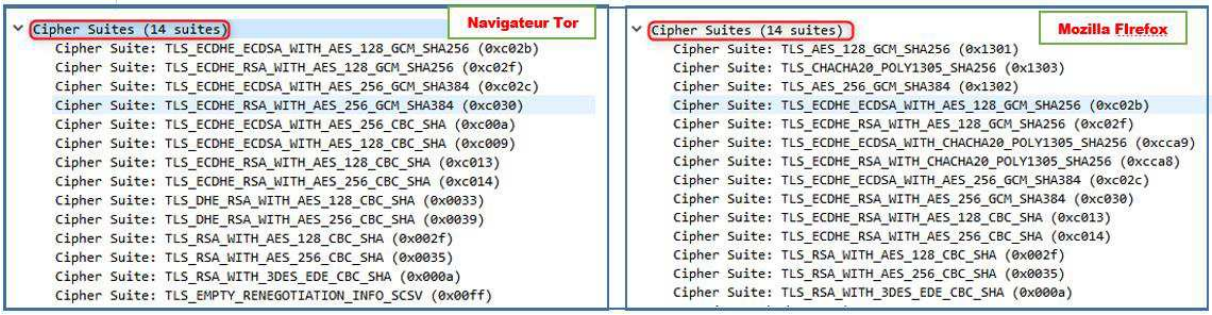

Figure 3.15: Les suites de chiffrement proposé par navigateur Tor et Mozilla Firefox.

Navigateur Tor utilise 6 extensions dans le message Client hello, par contre Google chrome utilise 17 extensions et Mozilla Firefox 13. Il y a des extensions communes entre les trois navigateurs, mais il y a quand même des différences entre ces extensions, plus une extension utiliser seulement par navigateur Tor.

‘’ **Les extensions :** un navigateur peut contenir plusieurs extensions et le nombre d’extensions est différent d’un navigateur à l’autre, les extensions peuvent contribuer à une meilleure sécurité. Elles peuvent agir comme un identifiant unique, car elles sont nombreuses et disposent de nombreuses options. Les extensions permettent à un client de spécifier le nom du serveur auquel il souhaite se connecter. Elles peuvent fournir des informations supplémentaires si l'adresse IP héberge plusieurs pages Web ou des informations de chiffrement [23]. ’’

Les extensions qui nous intéressent sont encadrées en rouge dans la [figure 3.16] et l'extension utilisée seulement par navigateur Tor est encadrée en bleu.

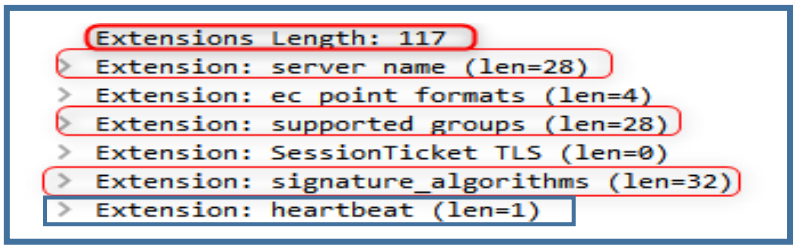

Figure 3.16: Les extensions utiliser par navigateur Tor

1- Extension « signature_algorithms » : cette extension contient les algorithmes de hachage supporter par le navigateur. Navigateur Tor propose 15 algorithmes de signature et Google chrome propose pour la même extension 14 algorithmes, Mozilla Firefox 11 algorithmes.

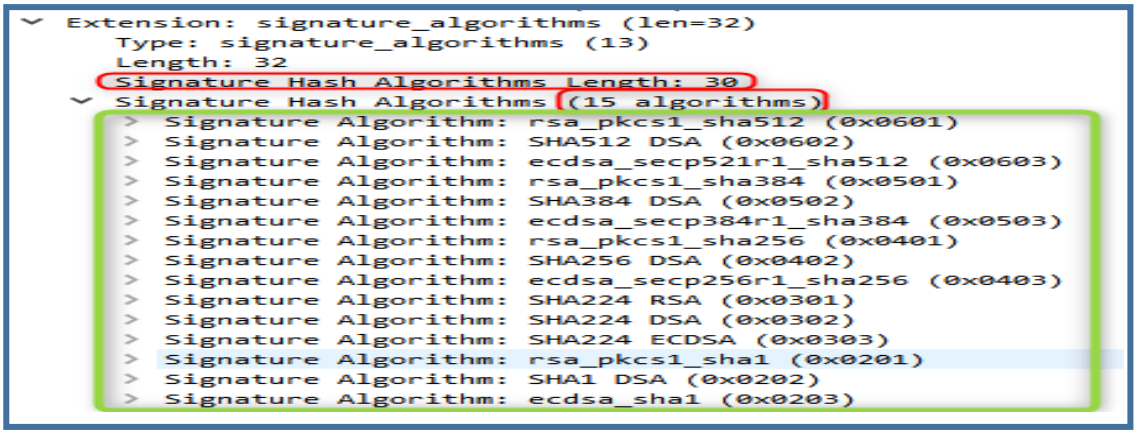

Figure 3. 17: Extension sinature_algorithms envoyer par navigateur Tor.

2- Extension Supported_Groupe : cette extension est utilisée pour les négociations de FFDHE (L'algorithme Diffie-Hellman est un algorithme d'échange de clés [26]). Navigateur Tor support 13 groupes, par contre Google chrome support « 4 groupes » et Mozilla Firefox « 6 groupes ».

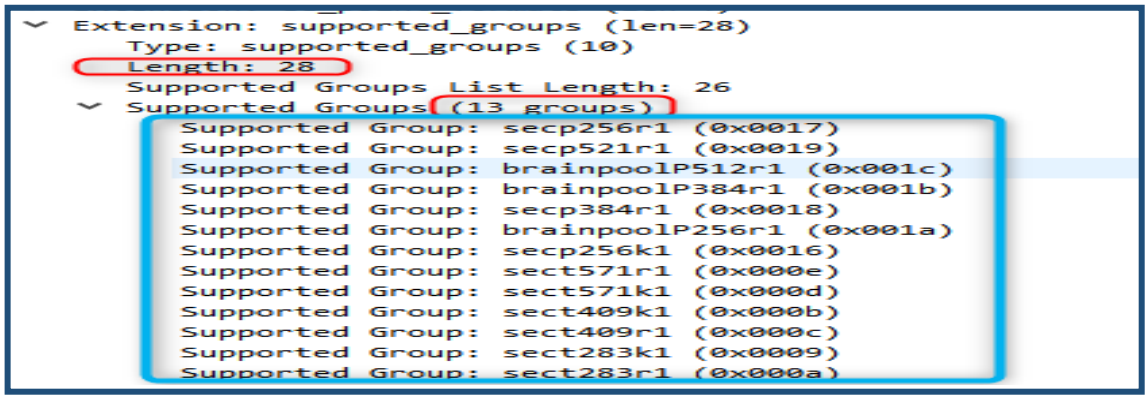

Figure 3.18: Extension Supported_groups envoyer par navigateur Tor

3- Extension server_name : cette extension est utilisée par le client pour spécifier au tout début de la négociation le nom du serveur auquel il souhaite se connecter. Dans cette extension on trouve le nom de domaine de serveur web de destination. Dans le cas de navigateur Tor on trouve un URL générer de façon aléatoire, par exemple : www.jznsim33mn6cgl.com.

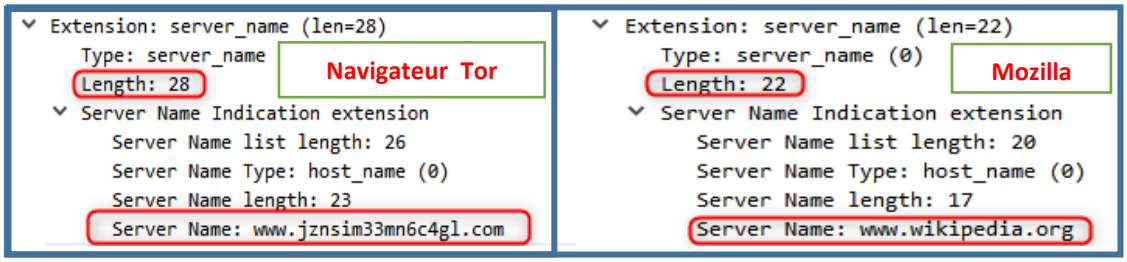

Figure 3. 19:Extension server_name.

Le nom de domaine délivrer dans l'extension serve_name de navigateur Tor n'appartient à aucun serveur :

Figure 3. 20: Nom de domaine généré par navigateur Tor.

4- Extension Heartbeat : elle est utilisée pour maintenir la connexion en vie sans transfert continu des données. Cette extension est utilisée seulement par le navigateur Tor, parce qu'il a besoin de garder la session sécurisée avec le nœud d'entrée du réseau Tor tout au long d'utilisation de l'application.

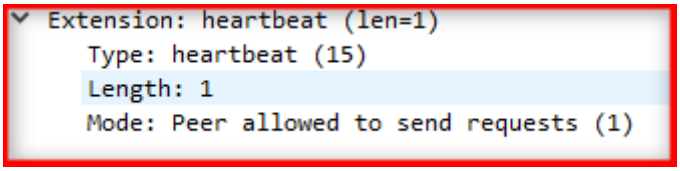

Figure 3. 21: Extension heartbeat.

b) Message Serveur Hello :

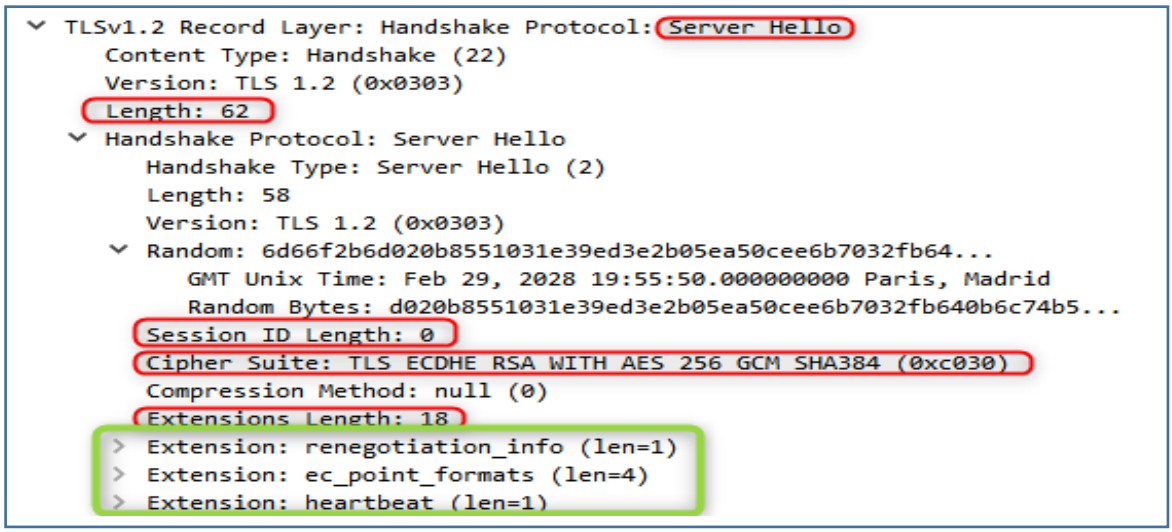

Figure 3. 22: Message Serveur Hello envoyé nœud d'entrée Tor.

Les suites de chiffrement choisi par les serveurs sont mentionnées dans le tableau suivant :

Serveur destination	Suit de chiffrement
nœuds d'entrées (1)	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
nœuds d'entrées (1)	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
nœuds d'entrées (1)	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
www.wikipédia.org	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
www.microsoft.com	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
www.w3schools.com	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA384
www.netacad.com	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Tableau 3.5 : Les suites de chiffrement.

La suite de chiffrement utilisée par les nœuds d'entrées Tor.

« TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ». celle-là se traduit par l'utilisation de TLS (non SSL), de Diffie-Hellman et de RSA pour le cryptage asymétrique. Il utilise ensuite AES_256_GCM avec une clé de 256 bits dans le mode de chiffrement par chaînage de blocs, pour le cryptage symétrique, SHA384 pour la vérification de l'intégrité des données. Cette suite est utilisée par plusieurs serveurs web.

Nœud d'entrée Tor utilise trois extensions dans le message serveur hello, par contre les autres serveurs web utilisent cinq extensions ou plus. Les deux premières extensions de serveur Hello de nœud Tor, sont utilisées par les autres serveurs web et il y n'a aucune différence entre eux, la troisième extension est « heartbeat » utilisée seulement par navigateur Tor.

Message Certificate, Certificate Status, Serveur Hello Done :

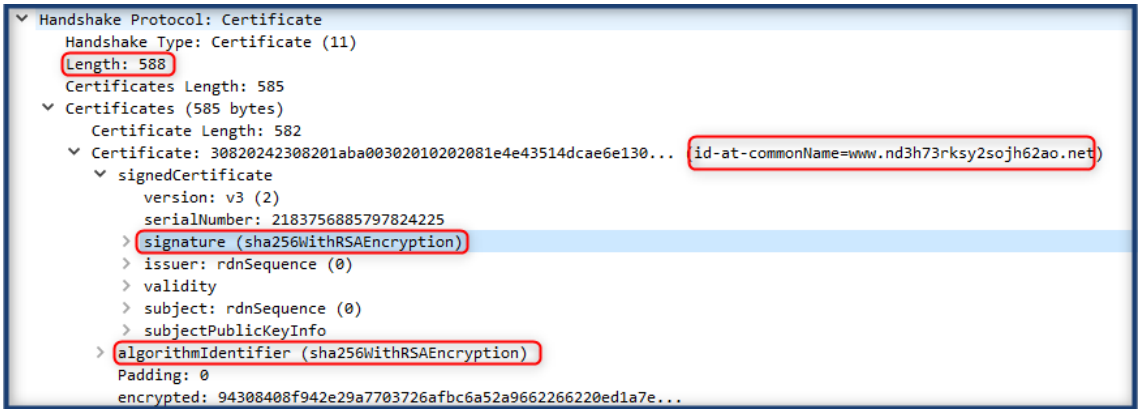

Figure 3. 23: Message Certificate envoyer par nœud d'entrée Tor

La longueur totale du message « certificat » envoyée par le premier nœud du Tor est trop petite (égale à 588 octets), par rapport à la longueur de message certificat envoyer par les autres serveurs web qu'elle est généralement supérieure de 3000 octets.

Le message « certificat » envoyée par les serveurs web contient deux certificats, le premier est celui de serveur web, le second est celui de l'autorité de certification (CA) qui a signé le premier certificat [la figure 3.24], par contre le message envoyer par nœud Tor contient un seul certificat générer et signer par le serveur lui-même (certificat auto-signer). Le nom de domaine délivré dans le certificat de serveur Tor est généré d'une façon aléatoire (voire la figure 3.24).

Figure 3.24: Message certificat envoyer par serveur Wikipedia.org.

La durée de validité de certificat de nœud Tor est généralement entre 294 jours et 300 jours. Il y a plusieurs serveurs web ont un certificat avec une durée de validité similaire. Par exemple la durée de validité de certificat de Wikipédia.org est 299 jours.

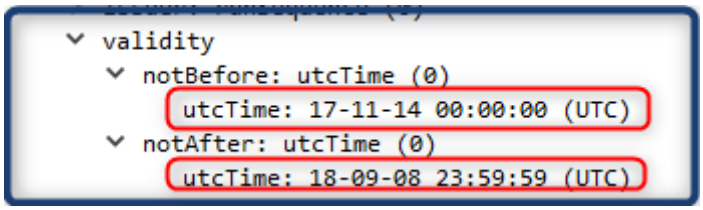

Figure 3. 25: Durée de validité de certificat de nœud Tor.

Constatation :

Les résultats de cette analyse, nous permettent de constater qu'il y a plusieurs différences qui peuvent distinguer l'utilisation navigateur Tor, par rapport aux autres navigateurs dans les paquets TLS de protocole d'établissement de connexion SSL « SSL handshake ». Nous allons utiliser ces différences pour extraire des empreintes numériques qui identifies réseau Tor. Afin de l'implémenter dans un système de détection d'intrusion réseau Snort. Pour cela, on était obligé d'étudie Snort et son fonctionnement, paramétrage et ces méthodes écriture des règles.

3.4 Système de détection d'intrusion :

a) Définition :

Les IDS, ou systèmes de détection d'intrusions, sont des systèmes software ou hardware conçus afin de pouvoir automatiser la surveillance d'événements survenant dans un réseau ou sur une machine particulière, et de pouvoir signaler à l'administrateur système, toute trace d'activité anormale sur ce dernier ou sur la machine surveillée. L'IDS est un système de détection passif [24].

IDS est un mécanisme destine à repérer des activités anormales ou suspecte sur la cible analysée, il permet d'avoir une connaissance sur les tentatives d'intrusions réussies et échouées.

b) Les fonctions d'un IDS :

Un IDS à quatre fonctions principales :

- **L'analyse :** il y a deux méthodes d'analyse, l'un est basé sur les signatures d'attaques, et l'autre sur la détection d'anomalie.

- **Journalisation :** enregistrement des évènements dans un fichier log exemple des évènements tentative de connexion.

- **Gestion :** les IDS doivent être administrés d'une façon permanente.

- **Action :** alerte l'administrateur lorsqu'une tentative d'intrusion est détectée.

c) Les types des IDS :

Il existe plusieurs types d'IDS, mais on peut les classer en trois familles principales :

- **IDS réseau NIDS :** les NIDS sont dédiés aux réseaux, ils analysent et interprètent les paquets circulant sur le réseau. Ils sont implémentés de la façon suivant : les sondes (les captures) sont placées aux endroits stratégiques du réseau et génèrent des alertes s'ils détectent une tentative d'intrusion. Ces alertes sont envoyées à une console sécurise qui les analyse et traitent.

- **IDS Host HIDS : l**es HIDS analysent le fonctionnement et l'état sur lesquelles ils sont installés, l'intégrité des systèmes et alors vérifie périodiquement et des alertes peuvent être déclenché.

- **Les IDS Hybride :** les IDS hybrides rassemblent les caractéristiques des NIDS et HIDS. Ils permettent, en un seul outil, de surveiller le réseau et les terminaux. Les sondes sont placées en des pointes stratégiques, et agissent comme NIDS et/ou HIDS suivant leur emplacement.

d) Modes de détection :

Il existe deux modes de détection :

La détection d'anomalie : elle consiste à détecter des anomalies par rapport à un profil du trafic habituel, la mise en œuvre comprendre une phase d'apprentissage au cours de laquelle les IDS découvrir le fonctionnement normal des éléments surveilles.

La reconnaissance des signatures : cette approche consiste à rechercher dans l'activité de l'élément surveille les empreintes (signature) d'attaque connues. Ce type d'IDS nécessite des mises à jour fréquentes.

Une signature permet de définir les caractéristiques d'une attaque, au niveau des paquets ou niveau protocole.

3.5 SNORT :

Snort est un système de détection d'intrusion libre pour le réseau (ou NIDS) publié sous licence GNU GPL. C'est également le cheval gagnant en matière de détection d'intrusion, utilisé par beaucoup d'entreprises et organisations gouvernementales. Snort est un des plus actifs NIDS Open Source et possède une communauté importante contribuant à son succès. Snort peut être configure pour fonctionner en trois modes :

Le mode sniffer : il lit les paquets circulant sur le réseau et les affiche sur l'invite de commande.

Le mode paquet logger : Snort journalise le trafic réseau dans des répertoires.

Le mode détecteur d'intrusion : Snort analyse le trafic réseau, compare ce trafic à des règles déjà définies par l'utilisateur et établi des actions à exécuter.

1- Modes de détection :

Il existe deux modes de détection :

La détection d'anomalie : Elle consiste à détecte des anomalies par rapport à un profil du trafic habituel, la mise en œuvre comprendre une phase d'apprentissage au cours de laquelle les IDS découvrir le fonctionnement normal des éléments surveilles.

La reconnaissance des signatures : Cette approche consiste à rechercher dans l'activité de l'élément surveille les empreintes (signature) d'attaque connues. Ce type d'IDS nécessite des mises à jour fréquentes.

2- Architecture de Snort :

L'architecture Snort est composée des éléments suivant :

Décodeur de paquet : il capture les paquets de données des interfaces réseaux, les prépare afin d'être prétraitées ou envoyées au moteur de détection.

Pre-processeur : ils reçoivent les paquets, les retraitent et les envoient au moteur de détection, ils sont utilisés afin d'améliore l'analyse.

Moteur de détection : il consiste à détecter les éventuelles intrusions qui existant dans un paquet, il consulte les règles et le compare avec le paquet de données. S'il y a conformité, le détecteur l'enregistre dans le fichier log et génère une alerte, sinon le paquet laisse tomber.

Système d'alerte et d'enregistrement des logs : il permet de génère les alertes et les messages log suivant ce que le moteur de détection a trouvé dans le paquet analyse.

Output modules : il permet de de traite l'intrusion génère par le système d'alerte et de notation de plusieurs manières : envoie vers un fichier log, génère un message d'alerte vers un serveur syslog, ou stocke cette alerte dans une base de données MySQL ou Oracl.

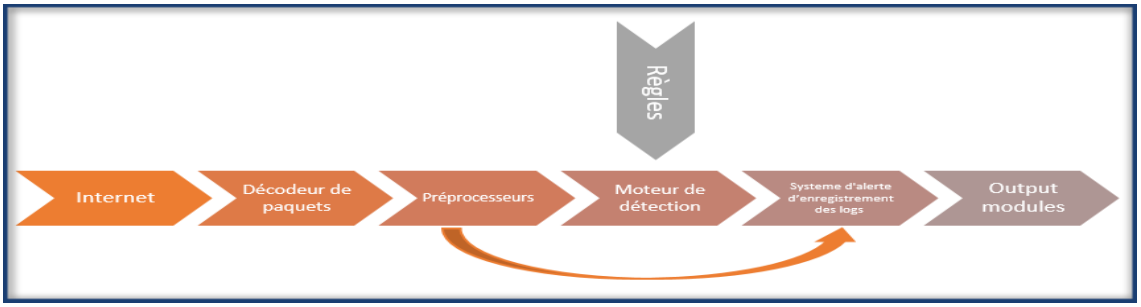

Figure 3. 26: Architecture de Snort

3- La conception des règles SNORT :

Les règles Snort sont compose de deux section logiques :

L'entête de la règle : contient comme information l'action de la règle, le protocole, les adresses IP source et destination, les ports source et destination, et les masque réseau.

Option de la règle : contient les messages d'alerte et les informations sur les parties du paquet qui doivent être inspectées pour déterminer si l'action de la règle va exécuter.

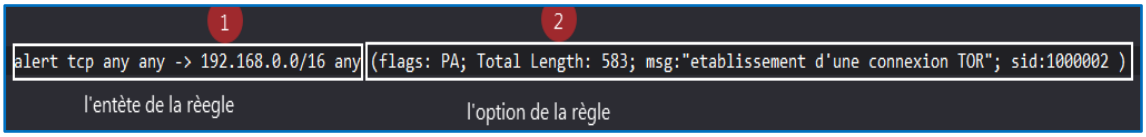

Figure 3.27: Les composent d'une règle Snort.

4- L'entête de règle :

L'action de règle : L'entête de règle contient l'information qui définit le "qui, où, et quoi" d'un paquet, ainsi que quoi faire dans l'événement où le paquet avec tous les attributs indiqués dans la règle devrait se présenter.

- **alert :** génère une alerte en utilisant la méthode d'alerte sélectionnée, et alors journalise le paquet [numéro 1 dans la Figure 3. 28].
- **log :** journalise le paquet
- **pass :** ignore le paquet
- **activate :** alerte et alors active une autre règle dynamic
- **dynamic :** reste passive jusqu'à être activée par une règle activate, alors agit comme une règle log.

Les protocoles : Il y a trois protocoles IP que Snort analyse actuellement pour des comportements suspicieux : tcp, udp, et icmp [numéro 2 dans la Figure 3. 28].

Les adresses IP : Les adresses IP source ou destination et on peut utiliser le mot clé **''ANY''** pour définie n'importe quelle adresse [numéro 3 dans la Figure 3. 28].

Les numéros de ports : Les ports source ou destination et on peut utiliser le mot clé **''ANY''** pour définie n'importe quel port [numéro 4 dans la Figure 3. 28].

L'opérateur de direction : L'opérateur de direction **"->"** indique l'orientation, **''->''** unidirectionnel, ou **<->** bidirectionnel [numéro 5 dans la Figure 3. 28].

5- Les options des règles :

Les options de règle forment le cœur du moteur de détection d'intrusion de Snort, combinant facilité d'utilisation, puissance et flexibilité. Voici quelques mots clé d'option de règle disponible dans Snort :

- **msg :** affiche un message dans les alertes et journalise les paquets [numéro 6 dans la Figure 3. 28].
- **logto :** journalise le paquet dans un fichier nommé par l'utilisateur au lieu de la sortie standard
- **id : identifié** le champ ID de fragment de l'entête IP pour une valeur spécifiée
- **fragbits :** identifié les bits de fragmentation de l'entête IP
- **dsize :** identifié la taille de la charge du paquet contre une valeur
- **flags :** identifié les drapeaux TCP pour certaines valeurs
- **seq :** identifié le champ TCP de numéro de séquence pour une valeur spécifique
- **ack :** identifié le champ TCP d'acquittement pour une valeur spécifiée
- **content :** recherche un motif dans la charge d'un paquet
- **content-list :**recherche un ensemble de motifs dans la charge d'un paquet
- **offset :** modifie l'option content, fixe le décalage du début de la tentative de correspondance de motif
- **depth** : modifie l'option content, fixe la profondeur maximale de recherche pour la tentative de correspondance de motif

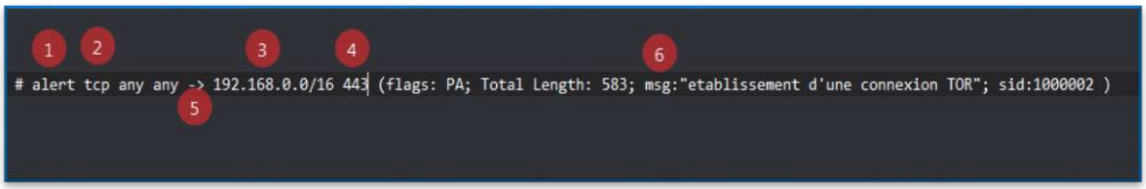

Figure 3. 28: Exemple d'une règle Snort

3.6 Extraction des empreintes digitales qui permettant l'identification du navigateur Tor et leurs implémentations dans Snort :

On a trouvé plusieurs identifiants de navigateur Tor au cours de notre expérimentation. Certains sont faciles à mettre en œuvre et à tester au niveau de Snort, tandis que d'autres sont difficiles à mettre en œuvre ou tout simplement irréalisables. Snort utilise les empreintes pour identifier le trafic malveillant. Pour que Snort puisse détecter Tor, on doit d'abord créer des empreintes qui déclenchent des alertes à l'utilisation de Tor. Ces empreintes doivent être créées par rapport aux fonctionnement et paramétrage de Snort pour qu'on puisse l'implémenter plus tard dans ce dernier. Pour ajouter de nouvelles empreintes à Snort on doit

créer une règle et Snort utilise un langage simple et léger de description de règles. Dans cette règle, on spécifie la direction du trafic et les octets qui identifient le trafic.

La première empreinte identifie les suites de chiffrement utilisées dans client Hello envoyé par navigateur Tor. Navigateur Tor propose 14 suite de chiffrement dans un ordre bien précis.

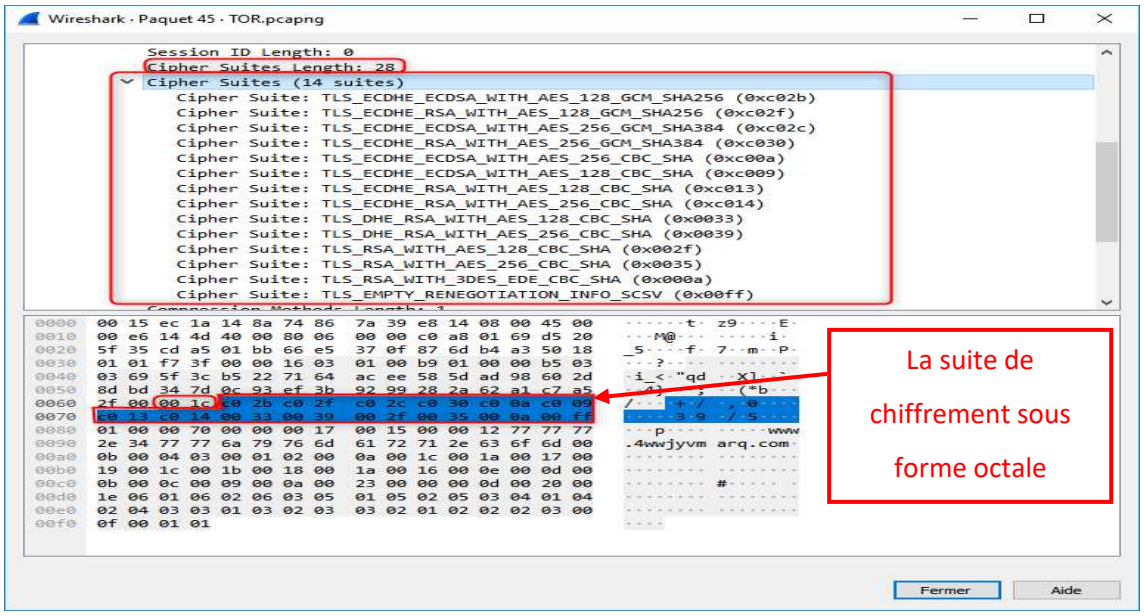

Figure 3. 29:L'empreinte des suites de chiffrement utilisées dans client Hello.

```
alert tcp any any -> any any (msg: "Possibilité d'utilisation de Tor: Suite de chiffrement
de cleint hello";  content:"|00 1c c0 2b c0 2f c0 2c c0 30 c0 0a c0 09 c0 13 c0 14 00 33 00
39 00 2f 00 35 00 0a 00 ff|"; offset:20; sid:100000008 ; rev:1;)
```

La deuxième empreinte identifie les groupes supporter utilisées dans client Hello envoyé par navigateur Tor. Navigateur Tor propose 13 groupes supporter .

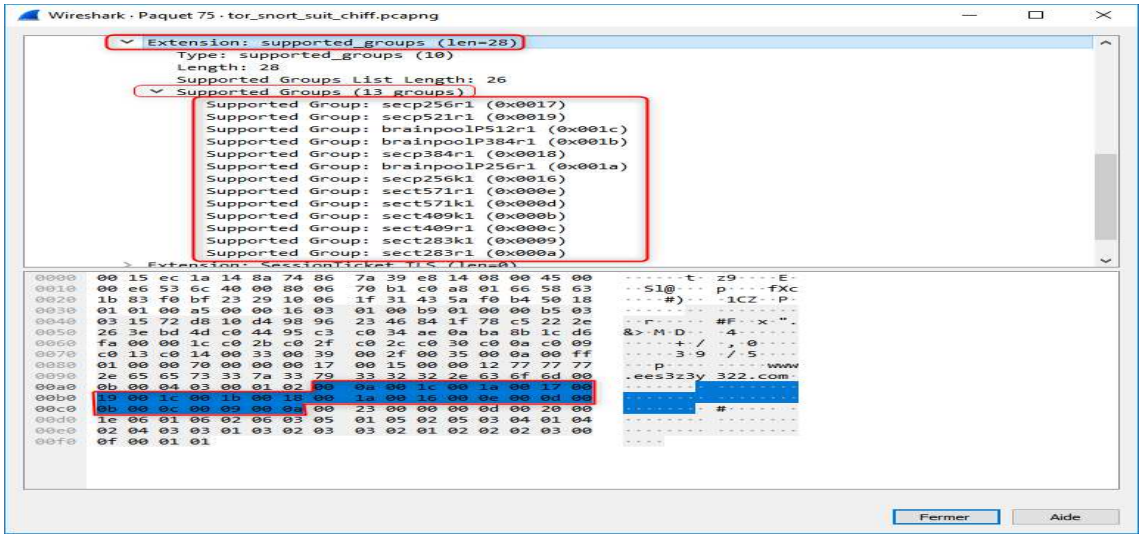

Figure 3. 30: L'empreinte de groupes supporter utilisées dans client Hello

```
alert tcp any any -> any any (msg: "Possibilité d'utilisation de Tor: Extension supported_g
roupe de cleint hello";  content:"|00 0a 00 1c 00 1a 00 17 00 19 00 1c 00 1b 00 18 00 1a 00
16 00 0e 00 0d 00 0b 00 0c 00 09 00 0a|"; offset:20; sid:100000010 ; rev:1;)
```

La troisième empreinte identifie les algorithmes de signatures utilisées dans client Hello envoyé par navigateur Tor. Navigateur Tor propose 15 suite de signatures.

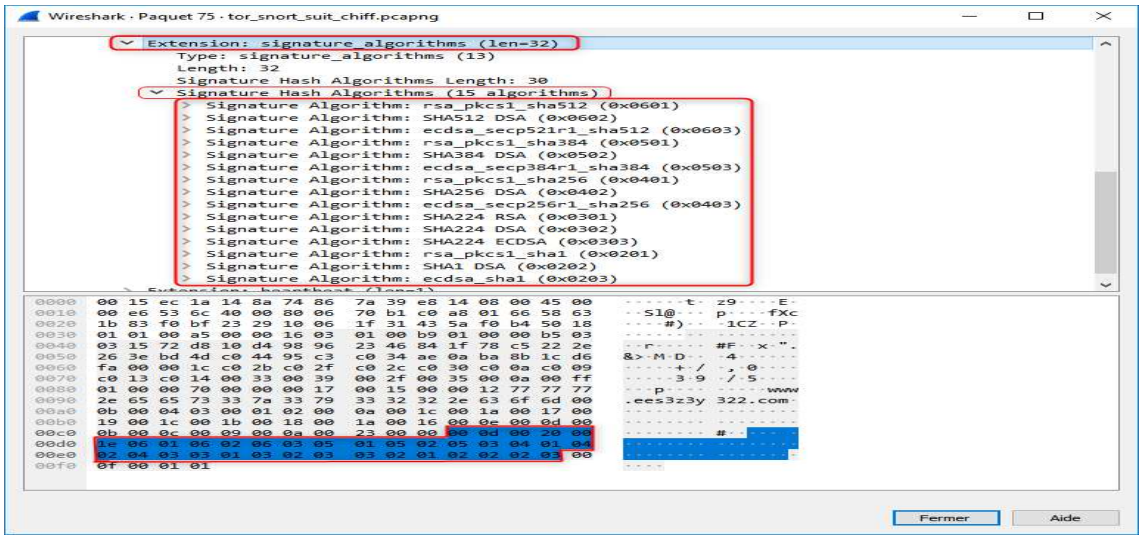

Figure 3. 31: L'empreinte de algorithmes désignateurs utilisées dans client Hello.

```
alert tcp any any -> any any (msg: "Possibilité d'utilisation de Tor: Extension signature_a
lgo de cleint hello"; content:"|00 0d 00 20 00 1e 06 01 06 02 06 03 05 01 05 02 05 03 04 01
04 02 04 03 03 01 03 02 03 03 02 01 02 02 02 03|";offset:20 ;sid:100000011 ;rev:1 ;)
```

La quatrième empreinte identifie l'extension heatbeat utilisée uniquement dans client Hello envoyé par navigateur Tor et Server Hello envoyé par les nœuds d'entrées Tor.

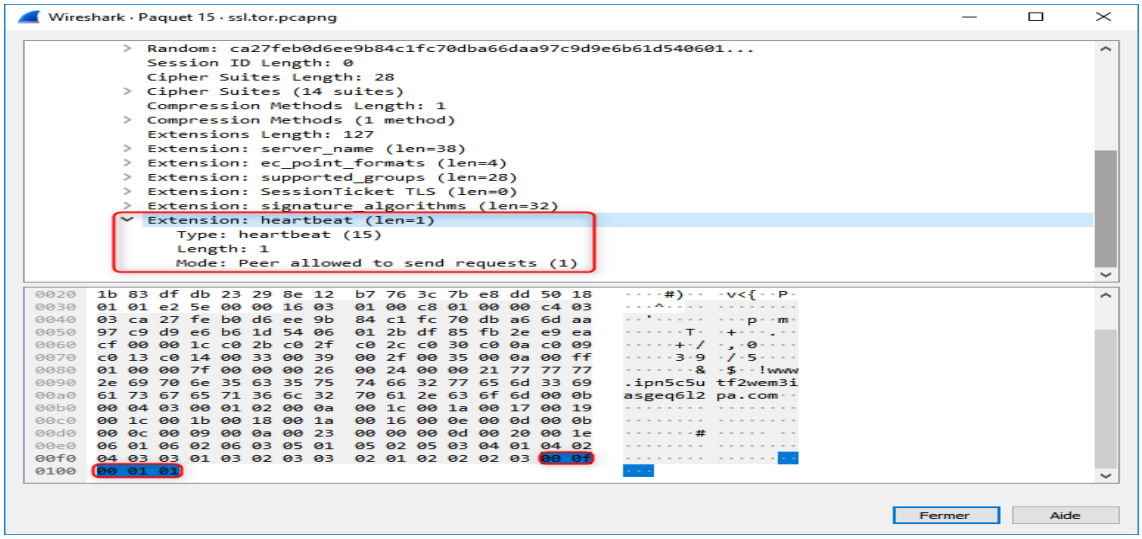

Figure 3. 32: L'empreinte de l'extension heatbeat.

```
alert tcp any any -> any any (msg: "Possibilité d'utilisation de Tor: Extension heartbeat "
; content:"|00 0f 00 01 01|"; offset:20; sid:100000012 ; rev:1;)
```

La cinquième empreinte identifie les ports (destinations) utilisées par les nœuds du réseau Tor, les ports les plus utilisés sont : les ports entre 9001 et 9010, le port 9030.

```
alert tcp any any -> any [9001:9010,9030] (msg:""Possibilité d'utilisation de Tor:Port dest
ination"; sid:100000013 ; rev:1; classtype:bad-unknown;) ##
```

La sixième empreinte identifie les adresses IP des nœuds du réseau Tor :

```
alert ( msg: "reputation: Packet is blacklisted"; sid: 1; gid: 136; rev: 1; metadata: rule-
type preproc ; classtype:bad-unknown; )
```

Cette dernière règle fonctionne à partir de version 2.9.1.0 de Snort. Parce que elle utilise le « Reputation Preprocessor » qui est inclus dans Snort à partir de cette version.

Le « Reputation Preprocessor » a été créé pour permettre à Snort d'utiliser un fichier contenant uniquement des adresses IP pour identifier les adresses IP malveillantes et les adresses IP de confiance. Les adresses IP malveillantes sont stockées dans un fichier des listes noires « black_lists » et les adresses IP de confiance sont stockées dans un fichier des listes blanches « white_lists ». Le « Reputation Preprocessor » charge ces listes au démarrage de Snort et compare les adresses du trafic avec les adresses de ces listes pour bloquer/laisser passer le trafic ou déclencher une alerte [27].

Nous avons ajouté la liste des adresses IP des nœuds du réseau Tor dans le fichier /etc/snort/rules/iplists/black_list.rules .

Pour ajouter nos règles à Snort, on a créé le fichier « /etc/snort/rules/local.rules », et on a ajouté nos règles dans ce fichier. Nous avons également édité le fichier snort.conf pour indiquer à Snort de charger le fichier « local.rules » (On a décommenter la ligne: include $ RULE_PATH / local.rules dans snort.conf). Lorsque Snort démarre, il utilisera le fichier de configuration snort.conf pour charger toutes les règles en local.rules.

3.7 Conclusion :

Dans ce chapitre, nous avons étudié le trafic web provenant du réseau Tor et celui de web normal, afin de faire une comparaison entre les deux. Nous avons montré qu'il existe plusieurs identifiants de navigateur Tor, surtout dans les paquets « Client Hello » et « certificat ».

Certains identifiants sont faciles à mettre en œuvre et à tester au niveau de Snort tandis que d'autre sont plus difficiles à mettre en œuvre ou tout simplement irréalisables. Pour l'implémenter dans Snort, nous avons proposé des règles basées sur certaines empreintes que nous avons trouvé.

Dans le quatrième chapitre, nous allons utiliser Snort pour tester la fiabilité de nos règles.

Chapitre 4 : Détection du réseau Tor

4.1 Introduction :

SNORT est un système de détection d'intrusion réseau (NIDS) open source qui fonctionne sur les systèmes Windows et Linux. Il permet d'analyser les flux de données en temps réel par rapport à une base de données de signature, mais aussi de détecter les anomalies.

Dans ce chapitre nous allons utiliser Snort pour détecter l'utilisation de réseau Tor. D'abord, nous allons exécuter Snort en tant qu'un système de détection d'intrusion réseau (NIDS), afin de tester nos différentes règles proposées dans le troisième chapitre.

4.2 Présentation de l'infrastructure de test :

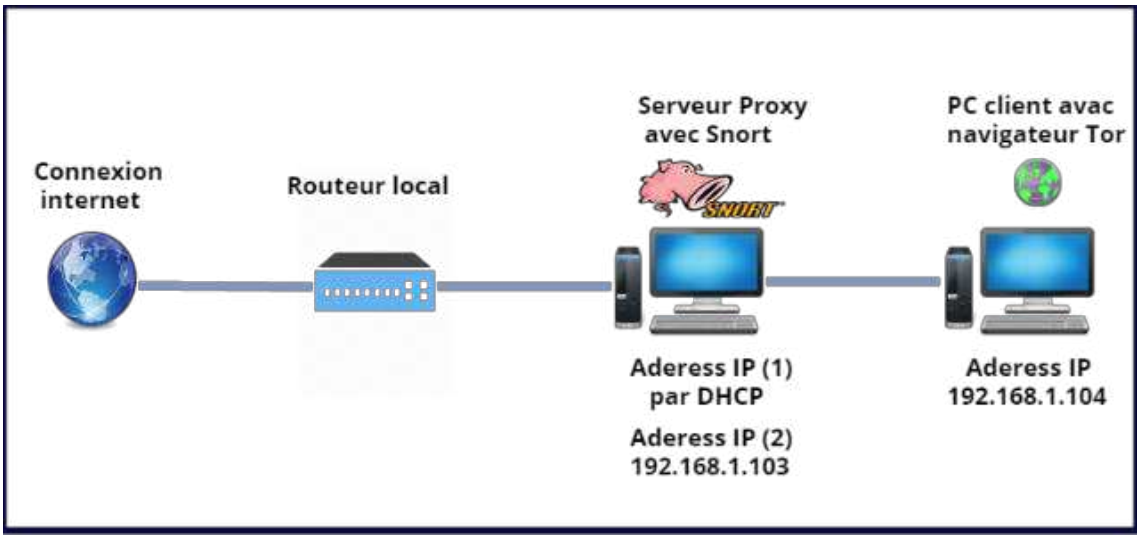

Figure 4. 1: L'infrastructure de test.

1- Sur PC1 :

Nous avons installé Snort version 2.8.6 avec une interface web BASE sous Windows 10 (la même version de Snort est installée dans le contre des systèmes et des réseaux d'information et de communication de l'université Saad Dahlab Blida 1). Cette version de Snort n'inclut pas «Reputation Preprocessor», pour tester ce dernier nous avons installé Snort 2.9.11.1 avec une interface web BASE sous Linux Ubuntu.

BASE (Basic Analysis and Security Engine) : est une interface web qui permet de visualiser les alertes générées par Snort. Ce dernier enregistrera les données d'alerte dans une base de données MySQL qui sera ensuite lue par BASE et affichée via un serveur web Apache.

- **Snort sous Windows est lancé avec les options suivantes:**

-i 3 : l'interface (3) à écouter.

-c /etc/snort/snort.conf : le chemin de fichier snort.conf.

-l : connexion au répertoire.

-K ascii : mode de journalisation (pcap [default], ascii, none)

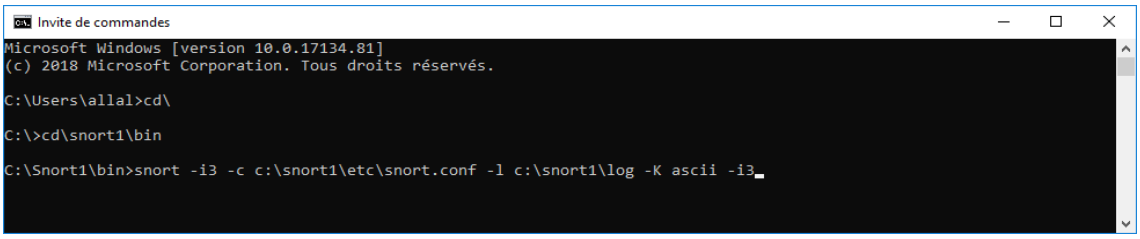

Figure 4. 2: Mise en marche de Snort sur Windows.

- **Nous avons utilisé deux lignes de commande pour fonctionner Snort sous Linux:**

1- La première ligne de commande pour lancer Snort avec les options suivantes :

```
sudo /usr/local/bin/snort -u snort -g snort -c /etc/snort/snort.conf -i enp70
```

-u snort -g : lancer Snort

-c /etc/snort/snort.conf : le chemin de fichier snort.conf.

-i enp70 : l'interface à écouter.

2- la deuxième ligne de commande pour lancer barnyard2 avec les options suivantes :

Barnyard2 : est interpréteur open-source pour les fichiers binaires de sortie de Snort de format unified2. Il permet de prendre en charge l'inscription des événements en base de données et libère donc des ressources à Snort qui peut davantage se concentrer sur la détection des intrusions [27].

```
sudo barnyard2 -c /etc/snort/barnyard2.conf -d /var/log/snort -f snort.u2 -w /var/log/snort/bar
nyard2.waldo -g snort -u snort
```

-c /etc/snort/barnyard2.conf : le fichier de configuration Barnyard2

-d / var / log / snort : l'emplacement pour rechercher le fichier Snort de sortie binaire

-f snort.u2 : le nom du fichier à rechercher.

-w /var/log/snort/barnyard2.waldo : le chemin vers le fichier waldo (fichier de point de contrôle).

-u Snort -g : exécuter Barnyard2.

2- Sur PC2 :

Nous avons installé les trois navigateurs : Tor, Mozilla Firefox, Google Chrome

4.3 Scenario de test:

La table ci-dessous représente les règles obtenus dans chapitre 3 :

Règle n°	Les règles
1	alert tcp any any -> any any (msg: "Possibilité d'utilisation de Tor: Suite de chiffrement de cleint hello"; content:"|00 1c c0 2b c0 2f c0 2c c0 30 c0 0a c0 09 c0 13 c0 14 00 33 00 39 00 2f 00 35 00 0a 00 ff|"; offset:20; sid:100000008 ; rev:1;)
2	alert tcp any any -> any any (msg: "Possibilité d'utilisation de Tor: Extension supported_groupe de cleint hello"; content:"|00 0a 00 1c 00 1a 00 17 00 19 00 1c 00 1b 00 18 00 1a 00 16 00 0e 00 0d 00 0b 00 0c 00 09 00 0a|"; offset:20; sid:100000010 ; rev:1;)
3	alert tcp any any -> any any (msg: "Possibilité d'utilisation de Tor: Extension signature_algo de cleint hello"; content:"|00 0d 00 20 00 1e 06 01 06 02 06 03 05 01 05 02 05 03 04 01 04 02 04 03 03 01 03 02 03 03 02 01 02 02 02 03|";offset:20 ; sid:100000011 ; rev:1;)
4	alert tcp any any -> any any (msg: "Possibilité d'utilisation de Tor: Extension heartbeat "; content:"|00 0f 00 01 01|"; offset:20; sid:100000012 ; rev:1;)
5	alert tcp any any -> any [9001:9010,9030] (msg:""Possibilité d'utilisation de Tor:Port destination"; sid:100000013 ; rev:1; classtype:bad-unknown;)
6 Sous Ubuntu	alert (msg: "reputation: Packet is blacklisted"; sid: 1; gid: 136; rev: 1; metadata: rule-type preproc ; classtype:bad-unknown;)

Tableau 4.1 : Les règles.

Pour tester la fiabilité de nos règles, on va voir ce scénario :

Nous avons décomposé notre test en deux parties. Dans la première partie, nous allons utiliser Snort sous Windows pour tester les cinq premières règles de la tableau 4.1.

D'abord on met en marche Snort sur le premier PC, ensuite dans le deuxième PC et on va lancer nos différents navigateurs pour accéder à plusieurs sites web. Dans le but de voir, si Snort peut détecter le réseau Tor, et d'une part, d'une autre s'il génère de fausses alertes (faux positifs).

Dans la deuxième partie, nous referons les mêmes étapes sous Ubuntu pour tester la sixième règle et « Reputation Preprocessor ».

4.4 Les résultats :

Une fois que nous avons connecté à BASE, la page principale affiche un résumé des alertes actuellement consignées ainsi que diverses ventilations du résumé des alertes et des liens vers les listes des alertes. Comme l'indique la figure 4.3, entre la fin de lancement de Snort et l'affichage de BASE, il y a eu déjà cinq alertes enregistrées, et cela sur le premier PC.

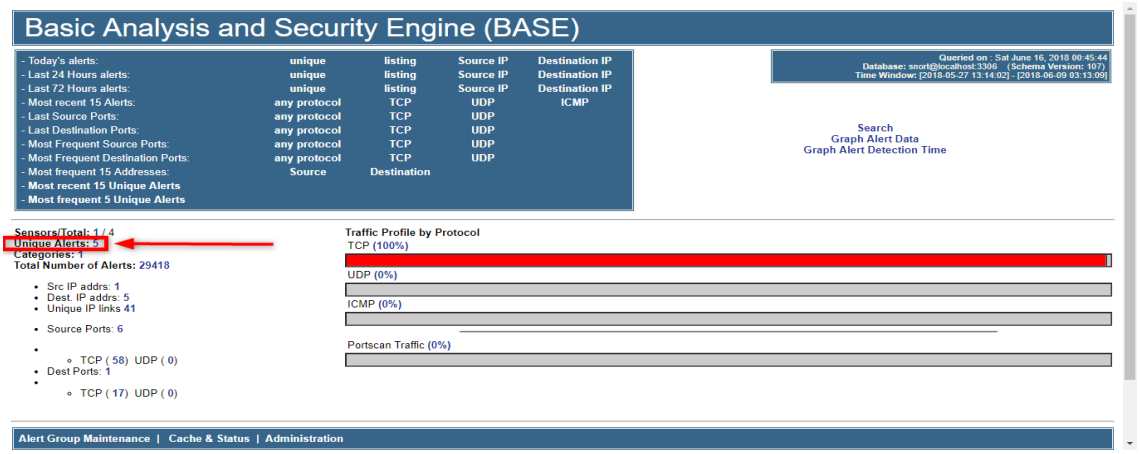

Figure 4. 3: L'interface principale de BASE.

Le lien « Unique Alerts » du tableau principal nous renvoie sur la liste des alertes.

BASE affiche, la signature indiquant le type d'alerte, ainsi que la date de déclenchement d'alerte.

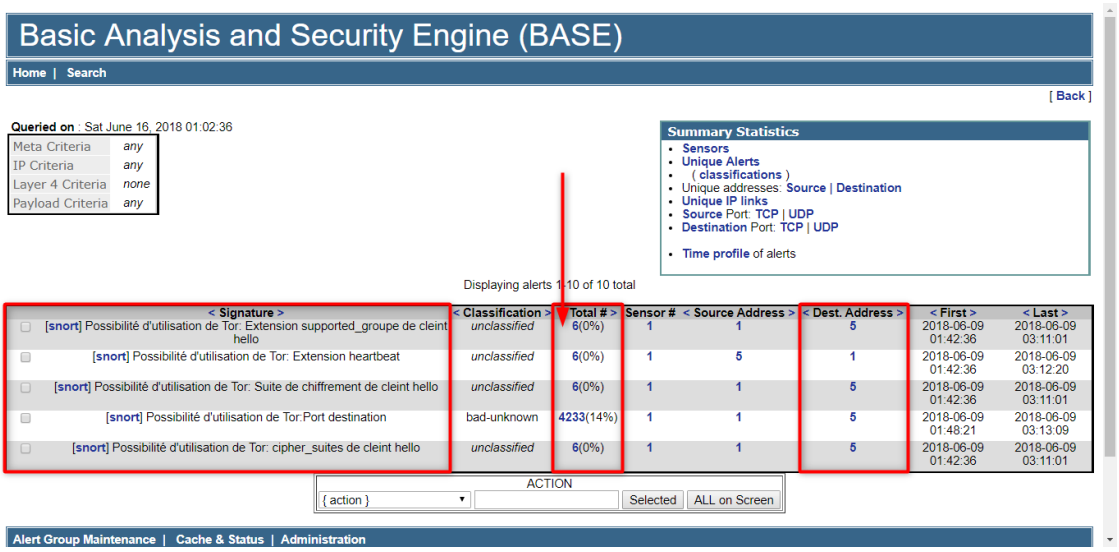

Figure 4. 4: Liste des alertes.

On remarque sur la figure 4.4 que Snort a détecté l'utilisation du navigateur Tor. Il a généré 5 alertes qui correspond à nos 5 règles. On remarque aussi que les alertes sont toutes déclenchées en même temps.

Le nombre total des alertes de chaque règle est 6, sauf la quatrième règle est 4233 alertes (nous allons expliquer cette différence plus tard dans ce chapitre) , lien « 6 » du la colonne « Total » nous renvoie sur la liste des alertes de chaque règle. On y apprend par exemple que la règle en question est « Extension supported_groupe de cleint hello », numéro 1 dans le tableau de BASE [figure 4.4].

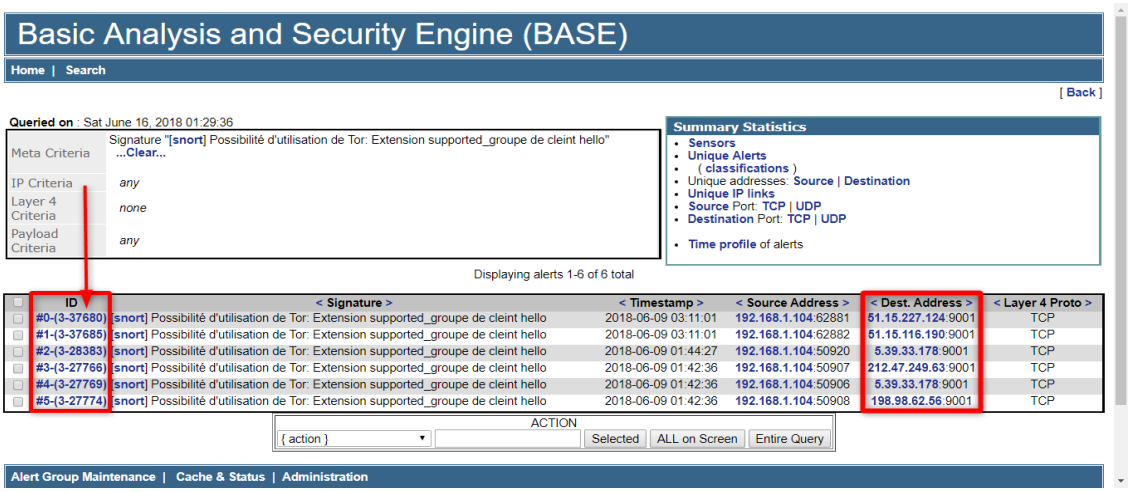

Figure 4. 5: Nombres d'alerte générer par la règle « Extension supported_groupe de cleint hello ».

BASE affiche, entre autres, l'adresse de destination et l'identifiant (numéro ID) de alerte. Dans le cas de [figure 4.5], on remarque que l'interface base affiche 6 alertes qu'elles correspondent à cette règle. Ces alertes indiquent 5 adresses destinations déférentes.

En cliquant à présent sur l'identifiant d'une alerte, BASE affiche les données complètes du paquet TCP/IP incriminé (en-tête IP, en-tête TCP, données du paquet TCP).

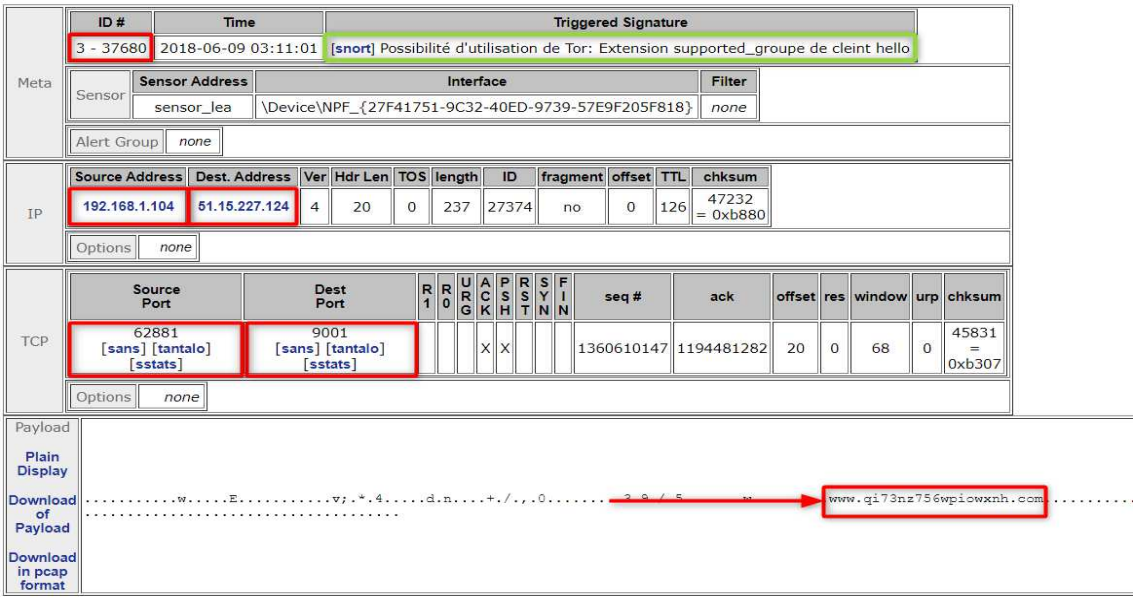

Figure 4. 6: L'alerte identifie par ID :37680

Dans figure 4.6, Nous pouvons extraire plusieurs informations sur l'alerte identifiée par ID :37680, entre autre, le nom de domaine «www.qi73nz756wpiowxnh.com» délivré dans le ce paquet. Il claire que ce nom de domaine est généré d'une façon aléatoire. Le nom de domaine délivré dans le paquet « Client Hello » envoyé par navigateur Tor est aussi généré d'une façon aléatoire.

Il existe un taux de faux positifs sur ce type d'alerte, il reste donc à vérifier le contexte de l'alerte afin de déterminer si l'on a bien affaire à une véritable tentative d'utilisation de réseau Tor ou juste un paquet qui ressemble à un paquet envoyé vers ou à partir de réseau Tor.

- Le nom de domaine aléatoire est un indice qui peut prouver l'utilisation de réseau Tor.

- Il est possible d'utiliser le site web : https://metrics.torproject.org /rs.html#search, pour vérifier si l'adresse de destination appartient au réseau Tor.

Les figures suivantes représentent les alertes générer par nos différentes règles :

1- Les alertes générées par la règle « les groupes supporter de Client Hello » :

Displaying alerts 1-6 of 6 total

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#0-(3-37680)	[snort] Possibilité d'utilisation de Tor: Extension supported_groupe de cleint hello	2018-06-09 03:11:01	192.168.1.104:62881	51.15.227.124:9001	TCP
#1-(3-37685)	[snort] Possibilité d'utilisation de Tor: Extension supported_groupe de cleint hello	2018-06-09 03:11:01	192.168.1.104:62882	51.15.116.190:9001	TCP
#2-(3-28383)	[snort] Possibilité d'utilisation de Tor: Extension supported_groupe de cleint hello	2018-06-09 01:44:27	192.168.1.104:50920	5.39.33.178:9001	TCP
#3-(3-27766)	[snort] Possibilité d'utilisation de Tor: Extension supported_groupe de cleint hello	2018-06-09 01:42:36	192.168.1.104:50907	212.47.249.63:9001	TCP
#4-(3-27769)	[snort] Possibilité d'utilisation de Tor: Extension supported_groupe de cleint hello	2018-06-09 01:42:36	192.168.1.104:50906	5.39.33.178:9001	TCP
#5-(3-27774)	[snort] Possibilité d'utilisation de Tor: Extension supported_groupe de cleint hello	2018-06-09 01:42:36	192.168.1.104:50908	198.98.62.56:9001	TCP

ACTION
Delete alert(s) | Selected | ALL on Screen | Entire Query

Figure 4. 7: Les alertes générer par la règle « les groupes supporter de Client Hello

2- Les alertes générées par la règle « suite de chiffrement de client Hello »:

Displaying alerts 1-6 of 6 total

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#0-(3-37681)	[snort] Possibilité d'utilisation de Tor: cipher_suites de cleint hello	2018-06-09 03:11:01	192.168.1.104:62881	51.15.227.124:9001	TCP
#1-(3-37686)	[snort] Possibilité d'utilisation de Tor: cipher_suites de cleint hello	2018-06-09 03:11:01	192.168.1.104:62882	51.15.116.190:9001	TCP
#2-(3-28384)	[snort] Possibilité d'utilisation de Tor: cipher_suites de cleint hello	2018-06-09 01:44:27	192.168.1.104:50920	5.39.33.178:9001	TCP
#3-(3-27767)	[snort] Possibilité d'utilisation de Tor: cipher_suites de cleint hello	2018-06-09 01:42:36	192.168.1.104:50907	212.47.249.63:9001	TCP
#4-(3-27770)	[snort] Possibilité d'utilisation de Tor: cipher_suites de cleint hello	2018-06-09 01:42:36	192.168.1.104:50906	5.39.33.178:9001	TCP
#5-(3-27775)	[snort] Possibilité d'utilisation de Tor: cipher_suites de cleint hello	2018-06-09 01:42:36	192.168.1.104:50908	198.98.62.56:9001	TCP

Figure 4. 8 : Les alertes générées par la règle « suite de chiffrement de client Hello

3- Les alertes générées par la règle « les algorithmes de signatures de Client Hello » :

Displaying alerts 1-6 of 6 total

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#0-(3-37679)	[snort] Possibilité d'utilisation de Tor: Extension signature_algo de cleint hello	2018-06-09 03:11:01	192.168.1.104:62881	51.15.227.124:9001	TCP
#1-(3-37684)	[snort] Possibilité d'utilisation de Tor: Extension signature_algo de cleint hello	2018-06-09 03:11:01	192.168.1.104:62882	51.15.116.190:9001	TCP
#2-(3-28382)	[snort] Possibilité d'utilisation de Tor: Extension signature_algo de cleint hello	2018-06-09 01:44:27	192.168.1.104:50920	5.39.33.178:9001	TCP
#3-(3-27765)	[snort] Possibilité d'utilisation de Tor: Extension signature_algo de cleint hello	2018-06-09 01:42:36	192.168.1.104:50907	212.47.249.63:9001	TCP
#4-(3-27768)	[snort] Possibilité d'utilisation de Tor: Extension signature_algo de cleint hello	2018-06-09 01:42:36	192.168.1.104:50906	5.39.33.178:9001	TCP
#5-(3-27773)	[snort] Possibilité d'utilisation de Tor: Extension signature_algo de cleint hello	2018-06-09 01:42:36	192.168.1.104:50908	198.98.62.56:9001	TCP

Figure 4.9: Les alertes générées par la règle « les algorithmes de signatures de Client Hello ».

4- Les alertes générées par la règle « l'extension Heartbeat » :

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#0-(3-37687)	[snort] Possibilité d'utilisation de Tor: Extension heartbeat	2018-06-09 03:11:01	51.15.227.124:9001	192.168.1.104:62881	TCP
#1-(3-37690)	[snort] Possibilité d'utilisation de Tor: Extension heartbeat	2018-06-09 03:11:01	51.15.116.190:9001	192.168.1.104:62882	TCP
#2-(3-28385)	[snort] Possibilité d'utilisation de Tor: Extension heartbeat	2018-06-09 01:44:28	5.39.33.178:9001	192.168.1.104:50920	TCP
#3-(3-27776)	[snort] Possibilité d'utilisation de Tor: Extension heartbeat	2018-06-09 01:42:36	212.47.249.63:9001	192.168.1.104:50907	TCP
#4-(3-27787)	[snort] Possibilité d'utilisation de Tor: Extension heartbeat	2018-06-09 01:42:36	5.39.33.178:9001	192.168.1.104:50908	TCP
#5-(3-27793)	[snort] Possibilité d'utilisation de Tor: Extension heartbeat	2018-06-09 01:42:36	198.98.62.56:9001	192.168.1.104:50906	TCP

Figure 4. 10: Les alertes générées par la règle « l'extension Heartbeat » .

5- Les alertes générées par la règle « liste des Ports de destination » :

Displaying alerts 1-48 of 4290 total

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#0-(3-40477)	[snort] Possibilité d'utilisation de Tor:Port destination	2018-06-09 03:13:09	192.168.1.104:62882	51.15.116.190:9001	TCP
#1-(3-40475)	[snort] Possibilité d'utilisation de Tor:Port destination	2018-06-09 03:13:09	192.168.1.104:62882	51.15.116.190:9001	TCP
#2-(3-40473)	[snort] Possibilité d'utilisation de Tor:Port destination	2018-06-09 03:13:09	192.168.1.104:62882	51.15.116.190:9001	TCP
#3-(3-40471)	[snort] Possibilité d'utilisation de Tor:Port destination	2018-06-09 03:13:09	192.168.1.104:62882	51.15.116.190:9001	TCP
#4-(3-40469)	[snort] Possibilité d'utilisation de Tor:Port destination	2018-06-09 03:13:09	192.168.1.104:62882	51.15.116.190:9001	TCP
#5-(3-40467)	[snort] Possibilité d'utilisation de Tor:Port destination	2018-06-09 03:13:09	192.168.1.104:62882	51.15.116.190:9001	TCP
#6-(3-40465)	[snort] Possibilité d'utilisation de Tor:Port destination	2018-06-09 03:13:09	192.168.1.104:62882	51.15.116.190:9001	TCP
#7-(3-40463)	[snort] Possibilité d'utilisation de Tor:Port destination	2018-06-09 03:13:09	192.168.1.104:62882	51.15.116.190:9001	TCP
#8-(3-40461)	[snort] Possibilité d'utilisation de Tor:Port destination	2018-06-09 03:13:09	192.168.1.104:62882	51.15.116.190:9001	TCP
#9-(3-40459)	[snort] Possibilité d'utilisation de Tor:Port destination	2018-06-09 03:13:09	192.168.1.104:62882	51.15.116.190:9001	TCP
#10-(3-40457)	[snort] Possibilité d'utilisation de Tor:Port destination	2018-06-09 03:13:09	192.168.1.104:62882	51.15.116.190:9001	TCP
#11-(3-40455)	[snort] Possibilité d'utilisation de Tor:Port destination	2018-06-09 03:13:09	192.168.1.104:62882	51.15.116.190:9001	TCP
#12-(3-40453)	[snort] Possibilité d'utilisation de Tor:Port destination	2018-06-09 03:13:09	192.168.1.104:62882	51.15.116.190:9001	TCP
#13-(3-40451)	[snort] Possibilité d'utilisation de Tor:Port destination	2018-06-09 03:13:09	192.168.1.104:62882	51.15.116.190:9001	TCP
#14-(3-40449)	[snort] Possibilité d'utilisation de Tor:Port destination	2018-06-09 03:13:09	192.168.1.104:62882	51.15.116.190:9001	TCP
#15-(3-40447)	[snort] Possibilité d'utilisation de Tor:Port destination	2018-06-09 03:13:09	192.168.1.104:62882	51.15.116.190:9001	TCP
#16-(3-40445)	[snort] Possibilité d'utilisation de Tor:Port destination	2018-06-09 03:13:09	192.168.1.104:62882	51.15.116.190:9001	TCP
#17-(3-40443)	[snort] Possibilité d'utilisation de Tor:Port destination	2018-06-09 03:13:09	192.168.1.104:62882	51.15.116.190:9001	TCP
#18-(3-40441)	[snort] Possibilité d'utilisation de Tor:Port destination	2018-06-09 03:13:09	192.168.1.104:62882	51.15.116.190:9001	TCP
#19-(3-40439)	[snort] Possibilité d'utilisation de Tor:Port destination	2018-06-09 03:13:09	192.168.1.104:62882	51.15.116.190:9001	TCP
#20-(3-40437)	[snort] Possibilité d'utilisation de Tor:Port destination	2018-06-09 03:13:09	192.168.1.104:62882	51.15.116.190:9001	TCP
#21-(3-40435)	[snort] Possibilité d'utilisation de Tor:Port destination	2018-06-09 03:13:09	192.168.1.104:62882	51.15.116.190:9001	TCP
#22-(3-40433)	[snort] Possibilité d'utilisation de Tor:Port destination	2018-06-09 03:13:09	192.168.1.104:62882	51.15.116.190:9001	TCP
#23-(3-40431)	[snort] Possibilité d'utilisation de Tor:Port destination	2018-06-09 03:13:09	192.168.1.104:62882	51.15.116.190:9001	TCP

Figure 4. 11: Les alertes générées par la règle « liste des Ports de destination »

6- Les alertes générées par la règle « liste des Adresses des nœuds Tor » (sous Ubuntu) :

Figure 4. 12 : les alertes capture par la règle « liste des Adresses des nœuds Tor ».

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#0-(1-50)	[snort] reputation: Packet is blacklisted	2018-06-09 23:35:29	192.168.1.104:42878	163.172.25.118:22	TCP
#1-(1-49)	[snort] reputation: Packet is blacklisted	2018-06-09 23:33:43	192.168.1.104:59446	37.120.191.245:9001	TCP
#2-(1-48)	[snort] reputation: Packet is blacklisted	2018-06-09 11:36:51	192.168.1.104:42098	163.172.25.118:22	TCP
#3-(1-47)	[snort] reputation: Packet is blacklisted	2018-06-09 11:36:43	192.168.1.104:42096	163.172.25.118:22	TCP
#4-(1-46)	[snort] reputation: Packet is blacklisted	2018-06-09 11:36:43	192.168.1.104:57950	82.220.89.53:9001	TCP
#5-(1-45)	[snort] reputation: Packet is blacklisted	2018-06-09 11:36:43	192.168.1.104:40600	51.15.80.59:9001	TCP
#6-(1-44)	[snort] reputation: Packet is blacklisted	2018-06-09 11:36:40	192.168.1.104:37008	193.11.114.43:9001	TCP
#7-(1-43)	[snort] reputation: Packet is blacklisted	2018-06-09 11:35:58	192.168.1.104:35856	37.120.191.245:9001	TCP
#8-(1-40)	[snort] reputation: Packet is blacklisted	2018-06-09 11:35:52	192.168.1.104:42864	195.154.164.243:443	TCP
#9-(1-39)	[snort] reputation: Packet is blacklisted	2018-06-09 11:28:42	192.168.1.104:42864	195.154.164.243:443	TCP
#10-(1-38)	[snort] reputation: Packet is blacklisted	2018-06-09 11:28:32	192.168.1.104:42860	141.255.166.189:443	TCP
#11-(1-37)	[snort] reputation: Packet is blacklisted	2018-06-09 11:28:32	192.168.1.104:42860	195.154.164.243:443	TCP
#12-(1-36)	[snort] reputation: Packet is blacklisted	2018-06-09 11:28:32	192.168.1.104:60066	51.15.13.245:8001	TCP
#13-(1-35)	[snort] reputation: Packet is blacklisted	2018-06-09 11:28:30	192.168.1.104:51338	163.172.149.155:443	TCP
#14-(1-32)	[snort] reputation: Packet is blacklisted	2018-06-09 11:27:42	192.168.1.104:35856	37.120.191.245:9001	TCP
#15-(1-31)	[snort] reputation: Packet is blacklisted	2018-06-09 11:25:09	192.168.1.104:42230	217.79.179.177:9001	TCP
#16-(1-30)	[snort] reputation: Packet is blacklisted	2018-06-09 11:25:00	192.168.1.104:42228	217.79.179.177:9001	TCP
#17-(1-29)	[snort] reputation: Packet is blacklisted	2018-06-09 11:25:00	192.168.1.104:42640	167.99.87.211:443	TCP
#18-(1-28)	[snort] reputation: Packet is blacklisted	2018-06-09 11:25:00	192.168.1.104:48628	51.254.96.208:9001	TCP
#19-(1-27)	[snort] reputation: Packet is blacklisted	2018-06-09 11:24:57	192.168.1.104:34728	212.51.134.123:9001	TCP
#20-(1-26)	[snort] reputation: Packet is blacklisted	2018-06-09 11:24:05	192.168.1.104:35856	37.120.191.245:9001	TCP

Figure 4.13: les alertes capture par la règle « liste des Adresses des nœuds Tor »

Constatation :

Après l'analyse de toutes les alertes générées par Snort :

Le tableau 4.2 représente les adresses source et destination mentionner dans les alertes :

< Timestamp >	< Source Address >	< Dest. Address >
2018-06-09 03:11:01	**192.168.1.104**:62881	**51.15.227.124**:9001
2018-06-09 03:11:01	**192.168.1.104**:62882	**51.15.116.190**:9001
2018-06-09 01:44:27	**192.168.1.104**:50920	**5.39.33.178**:9001
2018-06-09 01:42:36	**192.168.1.104**:50907	**212.47.249.63**:9001
2018-06-09 01:42:36	**192.168.1.104**:50906	**5.39.33.178**:9001
2018-06-09 01:42:36	**192.168.1.104**:50908	**198.98.62.56**:9001

Tableau 4. 2 : Les adresses source et destination mentionner dans les alertes.

A l'aide de site https://metrics.torproject.org /rs.html#search, Nous avons confirmé que ces adresses de destination appartiennent au réseau Tor et cela veut dire que les règles n'ont pas provoqué des fausses alertes (faux positifs).

On remarque aussi que le nombre des alertes généré par la règle « liste des Ports de destination » est très grand et cela est totalement normal parce que cette règle génère une alerte sur chaque requête qui passe à travers les ports désignés sur la règle. Par contre les autres règles génèrent des alertes uniquement sur les requêtes de Client Hello ou serveur Hello envoyer dans l'étape d'établissement de connexion.

Snort 2.9.11.1 a pu détecter l'utilisation de réseau Tor en utilisant « Reputation Preprocessor » à l'aide de la sixième règle.

De cette façon, on peut confirmer la fiabilité de nos règles.

Conclusion :

Dans ce chapitre, nous avons vu comment mettre en place et exécuter Snort en tant qu'un système de détection d'intrusion réseau (NIDS) sous Windows et sous Linux Ubuntu.

Dans un premier temps, Snort a démontré qu'il peut détecter l'utilisation du réseau Tor en temps réel à l'aide de nos différentes règles proposées dans le chapitre 3.

L'interface BASE offre de nombreuses fonctionnalités intéressantes qui facilitent l'accès aux alertes générées par Snort, Ainsi que l'analyse de ces derniers.

Il existe un taux de faux positifs sur ce type d'alerte, donc il est nécessaire de vérifier le contexte de l'alerte afin de déterminer si l'on a bien affaire à une véritable tentative d'utilisation de réseau Tor.

En basant sur leurs résultats expérimentaux, nous avons pu confirmer la fiabilité de nos règles.

Conclusion générale

L'utilisation du réseau Tor dans les entreprises n'est pas conseillée. En effet, l'utilisation de cet outil à partir d'un réseau d'entreprise peut exposer l'entreprise à divers risques de sécurité et à des problèmes judiciaires.

La détection du réseau Tor dans un réseau d'entreprise est très compliquée et nécessite une mise à jour permanente des règles de sécurité (adresses IP, empreintes, etc.). Les organisations et entreprises devraient envisager le déploiement de plusieurs solutions, afin d'augmenter les chances d'empêcher l'utilisation de Tor dans leur réseau d'entreprise.

SNORT est un système de détection d'intrusion réseau (NIDS) qui permet de détecter l'utilisation de réseau Tor par rapport à une base de données d'empreinte.

Ce thème de mémoire qui fait l'objet de notre étude, nous a permis d'approfondir nos connaissances dans le réseau informatique et ses protocoles, comprendre comment fonctionne le réseau Tor, d'avoir une idée plus claire sur l'importance d'analyse des données et également de découvrit le système de détection d'intrusion réseau Snort et son approche.

Dans la partie d'analyse de trafic, nous avons montré qu'il existe plusieurs identifiants du réseau Tor et nous avons implémenté certains de ces identifiants en tant qu'empreinte dans Snort. Dans la partie pratique, on a réalisé la mise en œuvre de Snort, suivi des différents tests d'évaluation réalisés. Ainsi Snort a démontré qu'il peut détecter l'utilisation de navigateur en temps réel à l'aide de nos différentes règles.

À partir de notre travail, on propose une liste de recommandation pour empêcher l'utilisation de réseau Tor dans une entreprise :

- Implémentations d'un système de détection d'intrusion réseau (NIDS), avec des mises à jours permanentes des règles de sécurité (adresses IP, empreintes, etc.) qui permet la détection de réseau Tor.

- Implémentations d'un système de détection d'intrusion machine (HIDS) au niveau des périphériques de l'entreprise, pour empêcher l'installation et l'exécution des applications du réseau Tor.

- Règlement sur l'utilisation de Tor : le règlement de sécurité de l'entreprise doit interdire impérativement l'utilisation de l'ensemble de réseau Tor sur les ressources de l'entreprise. Ce règlement doit être soutenu par des pénalités sévères pour avoir exécuté des applications du réseau Tor.

- La sensibilisation et la formation : tous les employés doivent être conscients des risques liés à l'utilisation du Tor dans leur réseau d'entreprises.

Finalement, les entreprises doivent empêcher aussi l'utilisation des serveurs Proxy web et les services VPN internet dans leur réseau, car ils peuvent être utilisés par les employés pour contourner la politique de sécurité de l'entreprise ou dans des activités malveillantes.

Bibliographie

[1] Cisco « Cisco Certified Network Associate 1 » version 6: Notions de base sur les réseaux.

[2] Réseaux Informatiques: Notions Fondamentales 3ème édition, Philippe ATELIN, eni éditions

[3] Initiation aux réseaux, Cours et exercices, Guy Pujolle, Eyrolles, 2001.

[4] [RFC 1122] Requirements for Internet Hosts – Communication Layers, https://tools.ietf.org/html/rfc1122.

[5] Cisco « Cisco Certified Network Associate 2 » version 6: Routage et commutation.

[6] Apprenez le fonctionnement des réseaux TCP/IP, Romain Guichard (Caelifer) , elalitte, openclassrooms, 16/04/2013.

[7] Architecture des réseaux, Danièle Dromard; Dominique Seret, collection Synthex, Eduction France.

[8] Tout comprendre à l'affaire Snowden, leparisien, T.D.L, 05 novembre 2017. http://www.leparisien.fr/.

[9] Article 19 : Le droit à l'anonymat en ligne, Free Word Center, London, 2015.

[10] [RFC 5246] The Transport Layer Security (TLS) Protocol. https://tools.ietf.org/html/rfc5246.

[11] Mieux comprendre les certificats SSL, thawte.tbs-certificats.com.

[12] MIEUX COMPRENDRE LES CERTIFICATS SSL, ssl-europa, 2016.

[13] TLS Handshake Protocol. https://msdn.microsoft.com/.

[14] Anonymat sur Internet, Protéger sa vie privée 2 éditons, Matrin Untersinger. 2015.

[15] L'anonymat dans le réseau Tor (The Second-Generation Onion) Brieuc Barthélemy, 2015-2016, université de Mons.

[16] Cisco « Cisco Certified Network Associate 4 version 6 »: Connexion des réseaux

[17] Tor: Overview, https://www.torproject.org/about/overview.html.en.

[18] The Tor Relay Guide, https://trac.torproject.org/projects/tor/wiki/TorRelayGuide.

[19] Tor: The Second-Generation Onion Router, Roger Dingledine, Nick Mathewson, Paul Syverson, 2004.

[20] L'ACTU SÉCU 18 XMCO | PARTNERS : LE CÔTÉ OBSCUR DE L'INTERNET, Janvier 2008.

[21] Risks Associated to Using Tor inside a Business Network, Hassane Oumsalem, Avril 2016, https://www.hitachi-systems-security.com.

[22] https://www.wireshark.org.

[23] [RFC 6066] Transport Layer Security (TLS) Extensions: Extension Definitions. https://tools.ietf.org/html/rfc6066.

[24] Les sondes de sécurité IDS/IPS, Thibault PALUD, Mars 2010, institut d'électronique et d'informatique Gaspard Monge.

[25] [rfc1750] Randomness Recommendations for Security. https://tools.ietf.org/html/rfc1750 .

[26] [RFC 7919] Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for Transport Layer Security (TLS), https://www.rfc-editor.org/rfc/rfc7919.txt.

[27] Barnyard2 https://doc.ubuntu-fr.org/barnyard2.

[28] The Reputation Preprocessor in Snort – Blacklists and Whitelists, Noah Dietrich, Snort Technology 2015. https://sublimerobots.com/2015/12/the-snort-reputation-preprocessor