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

en Télécommunication

Spécialité : Réseaux & Télécommunications

Présenté par

Ghermoul Samira.

&

Djeddi Hadjer.

Détection de l'usage du réseau anonyme JONDONYM dans un réseau d'entreprise.

Proposé par : Mr.Mehdi Merouane & Mlle.Amalou Warda.

Année Universitaire 2021-2022.

Remerciements

Au seuil de ce travail qui incarne la fin des études universitaires, on éprouve un réel plaisir à remercier tout ce qui nous ont aidé, directement ou indirectement, de près ou de loin à nous enquérir de la réalité des faits et nous ont guidé sur le droit chemin tout au long de la réalisation de notre mémoire de fin d'étude et à l'élaboration de ce travail, en l'occurrence notre encadreur Monsieur **MEHDI MEROUANE** pour la disponibilité dont il a fait preuve lorsque son aide et les informations concernant le mémoire étaient nécessaires.

Nos sentiments de gratitude s'adressent également à Mme **AMALOU WARDA** pour son suivi et ses conseils, ainsi que les jurys Mr **BENDOUMIA REDHA** et Mme **BOUTALEB** d'avoir accepté d'évaluer notre travail.

Enfin, nous tenons à exprimer toute notre gratitude à Mme. **FERGANI SOUAD** pour avoir relu et corrigé notre mémoire. Ses conseils de rédaction ont été très précieux, ainsi que son expérience professionnelle.

Nos vifs remerciements à tous nos enseignants durant les cinq années à l'université.

DEDICACES

Je dédié ce travail :

A mes très chers parents pour leur amour, leurs encouragements et leurs sacrifices et qui m'ont donné le gout de l'efforts et le sens de la responsabilité.

Je leurs dédie ce mémoire et mon diplôme en leur disant Merci du fond du cœur.

Je le dédie aussi à ma sœur Nihel Kenza mon petit frère Mohamed « MIMO », à mon cher fiancé SAMIR qui m'ont beaucoup supporté et encouragé

Mes amis, toute ma famille

et a tout ceux qui m'ont soutenue moralement au cours de la réalisation de ce projet .

GHERMOUL SAMIRA 🦋

Dédicaces

Je dédie ce travail, à mes chers parents, aucune dédicace ne saurait exprimer mon respect, mon amour pour les efforts qu'ils ont fourni pour mon instruction et mon bien être j'espère que je pourrais leurs rendre un peu de ce qu'ils ont fait pour moi un jour.

À mon cher oncle OMAR qui était toujours présent dans les moments difficiles

À mes sœur NAWEL et SOUMIA et mes amis Rochdi et YACINE, pour son soutient durant tout ce mémoire

Merci à vous

HADJER

ملخص: يسمح لنا هذا المشروع بكشف استعمال تطبيق أنون درويد لأجهزة أندرويد. ومتصفح جوندو براوزر تمرير بيانات تطبيقاته من خلال شبكة جوندونيم مما يتيح تغطية الأعمال غير القانونية مثل هجمات الكمبيوتر، وشراء وبيع المخدرات والأسلحة، الخ. من خلال الوصول إلى الشبكة المظلمة.

يتم كشف هذا التطبيق بمقارنة تدفق البيانات الخاصة به ببيانات الويب العادي لجمع بصمات رقمية تسمح بالتعرف على التطبيق. يتم وضع هذه البصمات الرقمية في نظام كشف التسلل ومنع اختراق الشبكات "سوريكاتا" لإطلاق تنبيه في كل محاولة للاتصال بهذا التطبيق.

كلمات المفاتيح: جوندونيم، جوندوبراوزر، بصمات رقمية، كشف، تدفق بيانات الويب، بصمات رقمية، نظام كشف التسلل ومنع اختراق الشبكات، سوريكاتا.

Résumé : L'utilisation des réseaux anonymes au sein des réseaux d'entreprises pour préserver l'anonymat sur Internet crée des canaux de communication cryptés permettant aux utilisateurs d'accéder aux parties les plus sombres de l'internet tel que le « DarkWeb » pour y mener des actions malveillantes. Ce projet consiste à détecter l'usage du réseau anonyme JonDonym dans un Réseau d'entreprise, en procédant à utiliser la technique de l'inspection approfondie des paquets "DPI". Ces paquets sont capturés préalablement à l'aide du logiciel "Wireshark" pour extraire les empreintes numériques du réseau JonDonym, qui seront ensuite implémentées à travers des règles personnalisées dans un système de détection d'intrusion "IDS Suricata" afin de déclencher une alerte à chaque tentative d'intrusion.

Mots clés : réseaux anonymes ; réseaux d'entreprises ; JonDonym ; DPI ; Wireshark ; IDS ; Suricata ; DarkWeb ; Proxy.

Abstract: The use of anonymous networks within enterprise networks to preserve anonymity on the Internet creates encrypted communication channels that allow users to access the darkest parts of the Internet, the "DarkWeb", to carry out malicious actions. This project consists in the detection of the use of the JonDonym anonymous network in an enterprise network, using the "DPI" deep packet inspection technique with the "Wireshark" software to extract the digital prints of the JonDonym network, which will be implemented by custom rules in an intrusion detection system "IDS Suricata" to trigger an alert at each intrusion attempt.

Keywords : Anonymous networks ; Enterprise networks ; JonDonym ; DPI ; Wireshark ; IDS ; Suricata ; DarkWeb ; Proxy.

Listes des acronymes et abréviations

LAN : Local Area Network.

WAN: Wide Area Network.

TCP: Transmission Control Protocol.

OSI: Open Systems Interconnection.

SYN: synchronized.

SYN-ACK: synchronize, acknowledge.

ACK: accusé de réception.

UDP: User Datagram Protocol.

TLS: Transport Layer Security.

SSL: Secure Socket Layer.

IP: Internet Protocol.

HTTP: HyperText Transport Protocol.

FTP: File Transfer Protocol.

DNS: Domain Name System.

IANA: Internet Assigned Numbers Authority.

NAT: Network Address Translator.

PAT: Port Address Translation.

ARP: Address Resolution Protocol.

ICMP: Internet Control and error Message Protocol.

DMZ: Zone démilitarisée.

TOR: THE ONION ROTING.

I2P: Invisible Internet Project.

JAP: Java Anon proxy.

DPI: Deep Packet Inspection.

IDS: Intrusion Detection System.

NIDS: Network Intrusion Detection System.

HIDS: Host-based intrusion detection system.

Table des matières

Liste des figures

Liste des tableaux

Introduction générale

Dans un monde connecté et ouvert, l'accès au DarkWeb à travers les réseaux anonymes constitue une source potentielle de plusieurs risques liés à la sécurité des systèmes informatiques et des personnes connectées. En effet, cette face cachée du Web est un faux ami. Elle commence par prôner une aspiration légitime celle d'un Internet non censuré ou la vie privée des utilisateurs est respectée et ses données personnelles protégées, pour virer ensuite sur une plateforme malveillante proposant des services nuisibles « Crime-as-a-Service (CaaS) ».

Interdire l'utilisation de ces réseaux anonymes au sein des entreprises est l'une des solutions permettant de renforcer la sécurité de leurs systèmes d'information. Elle nécessite une étude théorique approfondie sur les principes de fonctionnement des différents réseaux existant qui doit prendre en considération tous les paramètres, qu'ils soient matériels ou logiciels.

Avoir un système informatique sécurisé est aujourd'hui un réel défi pour les utilisateurs finaux et les entreprises au regard de l'utilisation accrue des services en ligne d'une part, et des nouveaux risques informatiques d'autre part ; Ainsi, c'est dans ce contexte, que le projet de fin d'études pour l'obtention de Master en réseau et télécommunication que nous allons réaliser a pour sujet : « Détection de l'usage du réseau anonyme JONDONYM dans un réseau d'entreprise ». La possibilité d'exercer nos compétences nous a donné l'opportunité de découvrir et d'enrichir nos connaissances dans le domaine de la sécurité informatique.

Via une vaste opération menée le 22/09/2020, l'agence européenne de police "Europol" a arrêté en Europe et aux Etats-Unis, 179 personnes soupçonnées d'avoir participé à des transactions illicites en utilisant le "DarkWeb", qui est l'un des points de concentration des plus grands criminels de la planète. [1]

Ainsi, ce coup de filet a mis en lumière sur les risques liés à la sécurité qui peuvent être provoqués par l'utilisation du réseau JONDONYM dans une entreprise. La question fondamentale suivante s'impose : La détection de l'utilisation du réseau JONDONYM dans une entreprise, est-elle possible ?

De cette problématique, s'enchaînent les questions suivantes :

- Qu'est-ce que l'anonymat et la vie privée sur Internet ?
- Quels sont les outils permettant l'anonymat ?
- Qu'est-ce qu'un réseau anonyme et quel est son mode de fonctionnement ?
- Qu'est-ce qu'un réseau JONDONYM ?
- L'implémentation des signatures du réseau JONDONYM dans un système de détection d'intrusion est-elle possible ?

Pour apporter des réponses adéquates à ce problème, nous avons mis en œuvre une solution qui consiste à analyser le trafic d'un réseau local pour détecter l'utilisation du réseau JonDonym au sein de ce dernier.

Cette analyse débute par le lancement du logiciel « Wireshark » qui permet de capturer les paquets transitant dans le réseau dans le but de les comparer en utilisant la technique l'inspection profonde des paquets « DPI ». Le résultat de la comparaison est utilisé pour extraire les empreintes numériques du réseau JonDonym, qui une fois obtenues, seront implémentées à travers des règles personnalisées dans un système de détection d'intrusion « IDS Suricata».

Pour ce faire, ce mémoire est organisé en trois chapitres comme suit :

Dans le premier chapitre, nous présentons succinctement et de manière générale les réseaux informatiques afin l'élargir et de consolider nos connaissances dans ce domaine.

Le deuxième chapitre est dédié aux questions liées à la vie privée et anonymat sur internet. Il porte également sur les différents outils permettant de garantir l'anonymat ainsi qu'une étude théorique détaillée sur le réseau anonyme JonDonym. Nous avons jugé utile d'inclure dans cette partie aussi la technique d'inspection approfondie des paquets qui sera utilisé dans la partie implémentation de la solution.

Le troisième chapitre est consacré à l'étude portant sur la détection du réseau anonyme JonDonym au sein du réseau d'entreprise, qui se fait à travers l'analyse des paquets capturés par Wireshark et l'extraction d'empreintes digitales après leur comparaison.

En dernier lieu on termine le mémoire par une conclusion générale.

Chapitre 1 Généralité sur les réseaux informatiques.

1.1 Introduction

Le monde est devenu aujourd'hui un petit village grâce à l'avènement des réseaux informatiques. Initialement destinés à la recherche pour relier quelques universités américaines, ils ont évolué de manière exponentielle pour devenir un outil indispensable de développement pour divers secteurs d'activités.

Par ailleurs, la généralisation de l'utilisation des différents types de réseaux a révélé de nouvelles menaces liées à la sécurité des systèmes informatiques auxquels il fallait faire face.

Ce chapitre nous permettra de faire la lumière de manière générale sur les réseaux informatiques en mettant l'accent sur les types des réseaux, leurs protocoles de communication, leurs architectures et leurs modes de fonctionnement.

1.2 Les réseaux informatiques

Un réseau informatique peut être défini comme un ensemble d'ordinateurs, d'imprimantes et d'autres équipements connectés (avec ou sans fil), dans le but de permettre les communications entre les appareils.

D'un point de vue technique, le réseau informatique désigne le processus de transport et d'échange de données entre des points appelés "nœuds.

. Les réseaux informatiques peuvent être classifiés en deux catégories principales, les réseaux locaux et entendus [2]

1.2.1 Local Area Network (LAN) et Wide Area Network (WAN)

Les réseaux locaux sont des moyens de communication permettant d'interconnecter des équipements informatiques et de partager certaines ressources (de calcul, de stockage, d'impression, etc.) dans des espaces limités à quelques centaines de mètres.

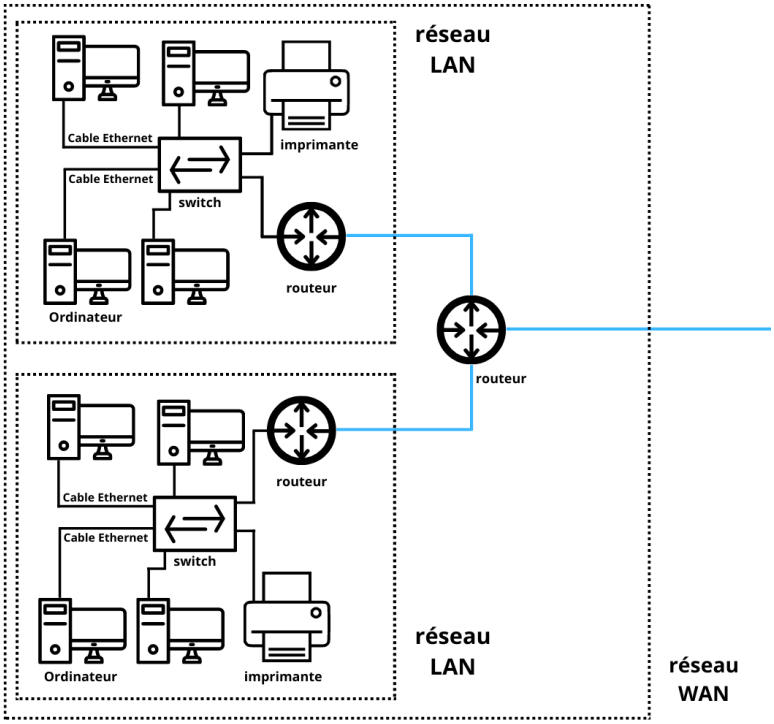

Figure 1: Architecture des réseaux LAN et WAN.

En revanche, les réseaux étendus (WAN) sont des réseaux qui couvrent un vaste territoire géographique, tel qu'une ville entière, une région ou même un pays. [3]

1.2.2 Intranet, Extranet et Internet

a Internet

Internet représente le plus grand réseau mondial permettant l'interconnexion de millions d'ordinateurs et serveurs. Nous pouvons à travers ce réseau envoyer des courriels, des photos, des vidéos et des messages à nos proches. Il crée un moyen de communication pour partager et obtenir des informations en ligne. Si votre appareil est connecté à l'internet, vous seul pourrez accéder à toutes les applications, sites web, applications de

médias sociaux et bien d'autres services. Internet est aujourd'hui considéré comme le moyen le plus rapide pour envoyer et recevoir des informations. [4]

b IntraNet

Le mot intranet est composé de deux mots : "Intra" signifie "à l'intérieur" et "net" signifie "réseau". La signification d'Intranet est donc "Réseau interne". La conception de l'Intranet est principalement destinée à la communication interne, car il s'agit d'un réseau privé auquel seuls les utilisateurs autorisés du réseau ont accès. Il existe de nombreux types de réseaux, dont certains se limitent à un réseau local (LAN), ce qui signifie que le système du réseau est relié par un fil LAN. D'autres sont accessibles à distance via l'intranet. [5]

c ExtraNet

Le réseau extranet est un sous-ensemble du réseau intranet. En d'autres termes, nous pouvons dire qu'il s'agit d'un réseau privé qui utilise la technologie Internet et le système de télécommunication public pour partager en toute sécurité des informations commerciales avec d'autres entreprises. L'extranet est décrit comme un "état d'esprit" et un moyen de faire des affaires avec d'autres entreprises et de vendre des produits aux clients. Ce réseau requiert sécurité et confidentialité et comprend la gestion de serveurs pare-feu, l'authentification de l'utilisateur (ici l'utilisateur est une autre entreprise). En utilisant ce réseau, le travail est effectué rapidement par rapport aux autres systèmes manuels. Il permet d'améliorer les relations avec les clients potentiels en leur fournissant des informations efficaces. [5]

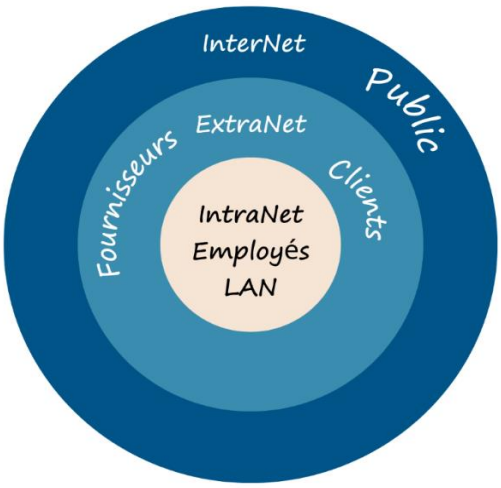

Figure 2: Intranet, Extranet et internet.

1.3 Le modèle TCP /IP

Le modèle TCP/IP est un modèle de référence en couches, c'est un modèle à quatre couches. Il est également appelé suite de protocoles Internet. Il est communément appelé TCP/IP car les protocoles de base sont TCP et IP, mais ces deux protocoles ne sont pas les seuls à être utilisés dans ce modèle. [6]

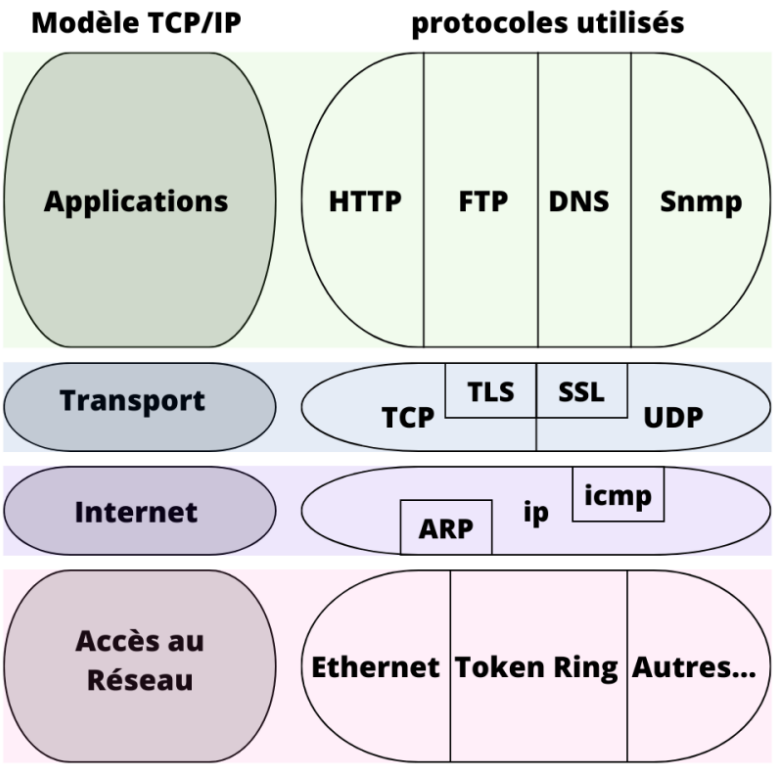

Figure 3: Architecture du modèle TCP/IP.

1.4 L'adoption du modèle TCP /IP entreprise

La série de protocoles TCP/IP présente plusieurs avantages : capacité à fonctionner sur des réseaux de différentes tailles, efficacité et évolutivité et indépendance par rapport à un constructeur ou un éditeur. Elle attire les entreprises qui se sont d'abord interconnectées via Internet, notamment pour la messagerie et les applications web.

Progressivement, elles ont aussi adopté ces protocoles standards de facto. Les intranets ont commencé à apparaître. Ils utilisent les mêmes protocoles et principes

qu'Internet, mais nécessite toutefois une authentification des employés de l'entreprise pour y accéder.

L'extranet désigne la possibilité pour un partenaire d'accéder à l'intranet local. En appliquant les mêmes règles au niveau du réseau, l'authentification reconnaît une personne extérieure à l'entreprise, dont les privilèges seront réduits

1.4.1 La couche application

La couche application du modèle TCP/IP fournit aux applications la possibilité d'accéder aux services des autres couches, et définit les protocoles que les applications utilisent pour échanger des données. [6]

- **HTTP, HyperText Transport Protocol,** assure le transfert de fichiers hypertextes entre un serveur Web et un client Web.
- **FTP, File Transfer Protocol,** est un système de manipulation de fichiers à distance (transfert, suppression, création...).
- **DNS, Domain Name System,** est un système de bases de données réparties assurant la correspondance d'un nom symbolique et d'une adresse internet (adresse IP).

1.4.2 La couche de transport

La couche de transport est chargée de fournir à la couche application des services de communication de session et de datagramme. Les protocoles de base de cette couche sont TCP et UDP. [6]

Le protocole de contrôle de transmission (TCP) est un protocole de transport qui fournit un service fiable et orienté connexion pour un flux d'octets.

- **Le protocole TCP :** utilise un mécanisme de poignée de main three way handshake) e mettons en œuvre 3 échange de segment (syn/syn ask/ask). Comme indiqué dans le schéma :

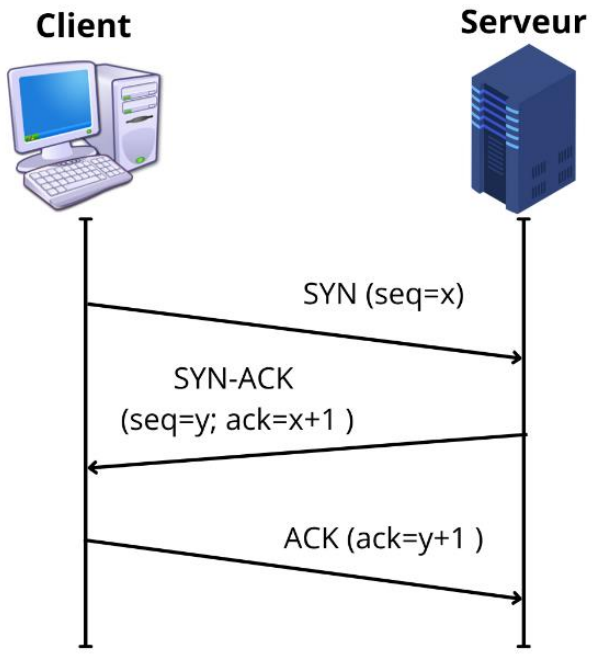

Figure 4: Diagramme de TCP Three Way Handshake.

- Le client envoie un paquet SYN (synchroniser) au serveur, qui a un numéro de séquence aléatoire.
- Le serveur renvoie un paquet SYN-ACK, contenant un numéro de séquence aléatoire et un numéro ACK accusant réception du numéro de séquence du client.
- Le client envoie un numéro ACK au serveur, accusant réception du numéro de séquence du serveur.
- Les numéros de séquence aux deux extrémités sont synchronisés. Les deux extrémités peuvent désormais envoyer et recevoir des données indépendamment.

- **User Datagram Protocol (UDP)** est un protocole de transport non orienté connexion. Il est donc très rapide mais surtout peu fiable.
- **TLS/SSL :** sont des protocoles de sécurité basé sur le chiffrement.il sont utilisé pour fournir des services de sécurité de base d'authentification, de confidentialité et d'intégrité des données sensible. Le SSL est le prédécesseur du chiffrement moderne TLS utilisé aujourd'hui.

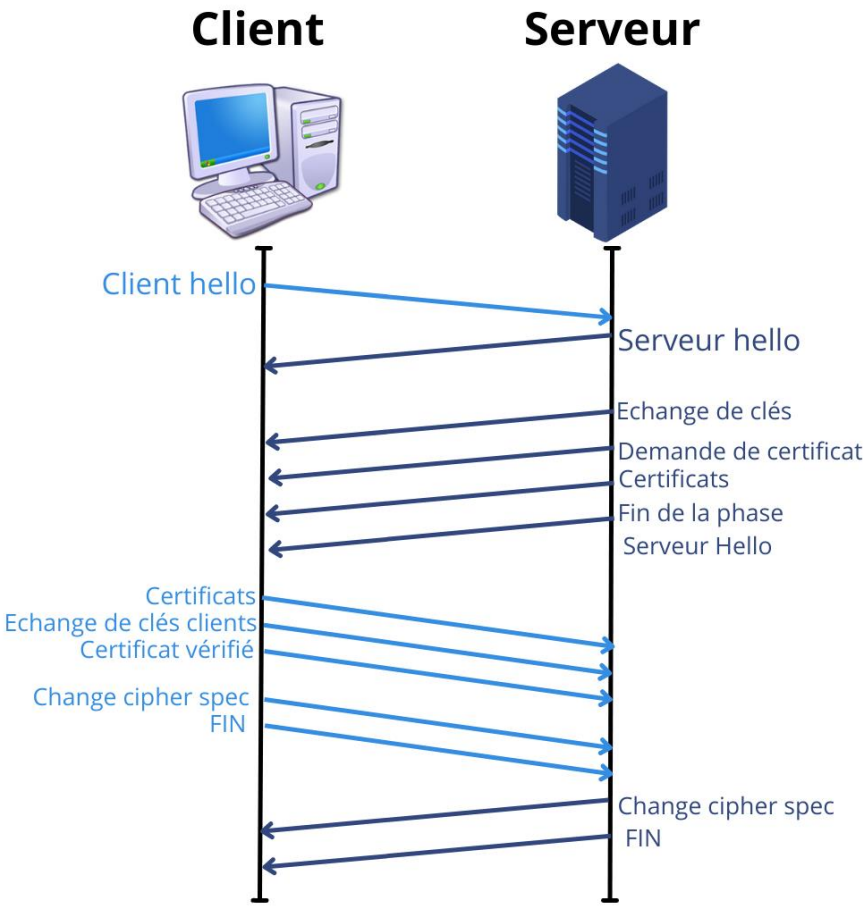

Figure 5: Diagramme de SSL Handshake.

Pour établir une connexion cryptée TLS/SSL, le client et le serveur effectuent l'ensemble des opérations suivantes :

1. Message « Client Hello » : le client démarre la négociation en envoyant un message « Hello » au serveur. Le message inclut la version TLS prise en charge par le client.
2. Message « Server Hello » : en réponse au message Client Hello, le serveur envoie un message contenant le certificat SSL du serveur.
3. Echange de clés : Message complémentaire pour l'échange des clés. Ce message contient la clé publique du serveur utilisée par le client pour chiffrer les informations de clé de session.
4. Demande de certificat : Demande un certificat au client pour l'authentifier.
5. Certificat : envoi d'une chaîne de certificats par le serveur. Le premier certificat est celui du serveur, le dernier est celui de l'autorité de certification.
6. Fin de phase serveur hello.

7. Certificat : Certificat éventuel du client si le serveur demande une authentification.
8. Echange de clés clients : Le client produit un secret pré-maître et le crypte avec la clé publique du certificat du serveur. Ces informations sont chiffrées une deuxième fois avec la clé publique du serveur.
9. Certificat vérifié : Message contenant une empreinte signée numériquement et créée à partir des informations de clé et de tous les messages précédents. Ce message permet de confirmer au serveur que le client possède bien la clé privée correspondante au certificat client.
10. Change Cipher Spec : Passage du client en mode chiffré avec la clé master comme clé symétrique.
11. FIN : Fin des émissions du client, ce message est chiffré à l'aide des paramètres de la suite de chiffrement.
12. Change Cipher Spec : Passage du serveur en mode chiffré avec la clé master
13. FIN : Confirmation au client du passage en mode chiffré. Ce message est chiffré à l'aide des paramètres de la suite de chiffrement.
14. Encrypted Data : Le tunnel SSL / TLS est établi, c'est maintenant le Record Protocol qui prend le relais pour chiffrer les données. [7]

1.4.3 La couche Internet

La couche Internet est responsable des fonctions d'adressage, de conditionnement et de routage des hôtes. Le protocole principal de la couche Internet est le protocole IP. [6]

- **Le protocole Internet (IP),** fournit un système de livraison de paquets sans connexion et non fiable. Il gère des adresses logiques, qui décomposent l'identifiant de chaque nœud en un numéro de réseau logique et un numéro de périphérique sur 4 octets (dans la version 4 du protocole IP).

a Adressage IP

1. Principe de l'adressage IP

IP fournit une livraison de paquets sans connexion et sans garantie. L'utilisation de TCP/IP nécessite que l'administrateur définisse un plan d'adressage, en prévoyant pour chaque nœud actif du réseau une adresse IP.

Celle-ci se compose de deux parties :

b Adresse IPv4

Une adresse IP version 4 est représentée sur 4 octets (32 bits). On utilise, pour cela, la notation décimale pointée, c'est-à-dire que chaque octet est affiché, séparé par un point : 192.168.1.1

Suivant la valeur du premier octet, il est possible de connaître la classe de l'adresse IP.

c Le masque

On utilise un masque de sous-réseau pour identifier la partie de l'adresse IP correspondant au réseau, de la partie identifiant le nœud. Si l'on écrit l'adresse IP en binaire, tous les bits associés au numéro de réseau vont être marqué d'un '1' dans le masque, d'un 'O' sinon.0

Tableau 1: Tableau d'adresse ipv4.

Classe	Masque réseau	Adresses réseau	Nombre de réseaux	Nombre d'hôtes par réseau
A	255.0.0.0	1.0.0.0 - 126.255.255.255	126	16777214
B	255.255.0.0	128.0.0.0 - 191.255.255.255	16384	65534
C	255.255.255.0	192.0.0.0 - 223.255.255.255	2097152	254

d Adressage privée et publique :

Pour permettre aux réseaux de s'interconnecter, il est nécessaire de s'assurer que les adresses sont uniques. C'est l'une des responsabilités de l'IANA, qui attribue une adresse unique à chaque réseau.

Une adresse attribuée par l'IANA est dite publique. Pour éviter une utilisation chaotique des adresses sur les réseaux privés, la réservation de la plage d'adresses de ces réseaux a été envisagée. Ces adresses ne peuvent pas être routées sur l'Internet, elles sont

réservées à un usage privé, et sont donc appelées adresses privées, tandis que les autres sont appelées publiques.

Tableau 2: Tableau d'adresse privée ipv4.

Classe	Masque réseau	Adresses réseau
A	255.0.0.0	10.0.0.0 - 10.255.255.255
B	255.255.0.0	172.16.0.0 - 172.31.255.255
C	255.255.255.0	192.168.0.0 - 192.168.255.255

e Network Address Translator (NAT)

Traducteur d'adresse réseau (NAT, Network Address Translator) est le processus par lequel une ou plusieurs adresses IP privées ou utilisateurs connectés à des réseaux LAN sont traduites en une ou plusieurs adresses IP publiques ou réseaux WAN et vice-versa pour fournir un accès à l'internet aux hôtes locaux. [8]

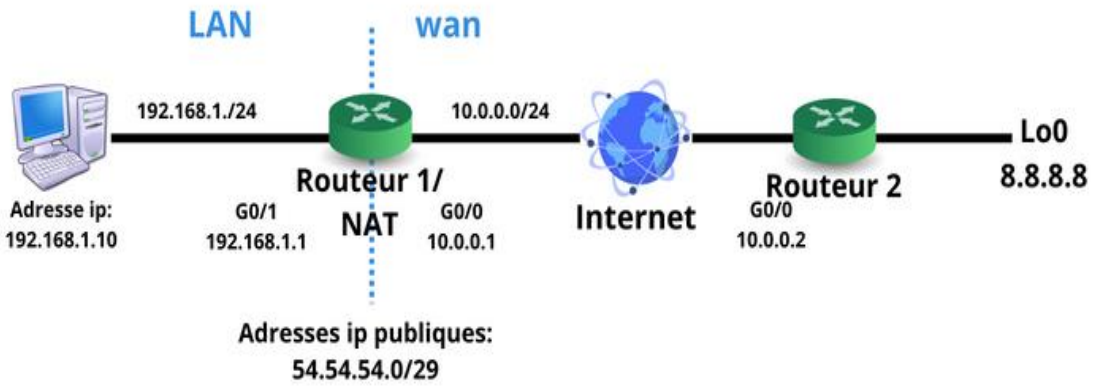

Figure 6: Principe du fonctionnement du NAT.

f Principe de fonctionnement du NAT

Lorsque le NAT doit être activé, un routeur doit être configuré, c'est-à-dire le routeur qui a une interface dans le réseau global (extérieur) et une autre interface dans le réseau local (intérieur) et lorsqu'un paquet traverse l'extérieur du réseau local, le NAT

convertit cette adresse IP locale (privée) en une adresse IP globale (publique) et inversement. [5]

Il existe trois différents types de NAT :

- **NAT statique :**

Le NAT statique est le type de base du NAT. Une adresse IP privée est convertie en une adresse IP publique. Ainsi, il ne peut cacher qu'une seule adresse IP privée. [9]

- **NAT dynamique :**

Le NAT dynamique est identique au NAT statique, mais ici nous avons un pool d'adresses IP publiques. Ainsi, il prend automatiquement une IP libre du pool d'IP publiques et modifie automatiquement l'en-tête IP du paquet.

Le NAT dynamique est utilisé dans les grands réseaux d'entreprise. Les grandes entreprises achètent une grande quantité d'adresses IP publiques et les conservent dans un pool. Ce pool est attribué à un groupe d'hôtes, et il commence à fournir des adresses IP publiques à ces hôtes. [9]

- **PAT (Port Address Translation) :**

Il s'agit d'un type de NAT. Il est utilisé pour fournir une connectivité Internet à un grand nombre d'hôtes en utilisant une seule adresse IP publique sur laquelle le port est modifié. Le PAT est largement utilisé dans les réseaux domestiques, de campus et d'entreprise. [9]

- **ARP, Address Resolution Protocol,** Mapper les adresses IP logiques sur une Adresse MAC physique (contrôle d'accès au support, adresse d'interface réseau Local)
- **ICMP, Internet Control and error Message Protocol,** Fournit un dialogue IP/IP, Inclut : signalisation des embouteillages, synchronisation de l'horloge et estimations Temps de transit ... utilisé par l'utilitaire ping pour tester son existence Depuis une station du réseau.

1.4.4 La couche d'accès au réseau

La couche d'accès au réseau est chargée de placer les paquets TCP/IP sur le support réseau et de recevoir les paquets TCP/IP du support réseau. [6]

1.5 Port logique

Le port réseau est un numéro unique qui est attribué à chaque application. Chaque protocole et adresse dispose d'un port, qui est désigné par un numéro de port.

Un numéro de port est un identifiant unique qui est utilisé en conjonction avec une adresse IP. Un port est un nombre entier non signé de 16 bits. Il y a 65 535 ports accessibles sous l'architecture TCP/IP. Internet Assigned Numbers Authority (IANA) est l'organisme standard chargé d'attribuer les numéros de port. [10]

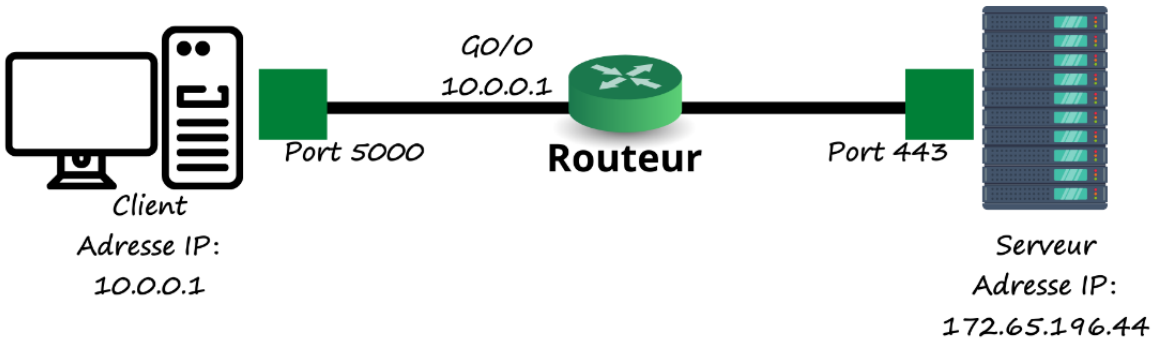

Figure 7: architecture client-serveur avec ports logique.

1.5.1 L'utilité des ports

Un même client peut avoir plusieurs connexions au même serveur ou à des serveurs différents. Plusieurs programmes peuvent être exécutés sur le client en même temps. Lorsque le client tente de contacter un service, l'adresse IP est insuffisante pour accéder au service. Le numéro de port est nécessaire pour accéder au service depuis un serveur. En attribuant un numéro de port aux applications, la couche transport joue un rôle important en favorisant différents canaux de communication entre ces applications. [10]

1.5.2 Classification des numéros de port

a Ports connus

La plage des numéros de port connus est de 0 à 1023. Les ports connus sont associés à des protocoles qui fournissent des applications et des services courants.

Si on veut, par exemple, accéder à certains sites Web sur Internet, on utilise le protocole HTTP disponible sur le numéro de port 80. [10]

Table 1: exemples de protocoles et leurs ports.

Protocole	N° de port
IP	4
UDP	17
TCP	6
SSH	22
FTP	20/21
HTTPS	443

b Ports enregistrés

Les ports enregistrés varient de 1024 à 49151. Les processus utilisateur utilisent les ports enregistrés. Les applications individuelles, par opposition aux applications standard avec un port connu, sont utilisées dans ces opérations. [10]

c Ports dynamique

Le port dynamique est compris entre 49152 et 65535. Lorsqu'un client établit une connexion, ces numéros de port sont donnés dynamiquement à l'application cliente. Lorsque le client commence la connexion, le port dynamique est identifié, alors que le port connu est connu avant la connexion. Aussi, lorsque le client se connecte au service, il n'a pas connaissance de ce port. [10]

1.6 Architecture client /serveur

L'architecture client/serveur désigne un mode de communication entre plusieurs composants d'un réseau. Chaque entité est considérée comme un client ou un serveur. Chaque logiciel client peut envoyer des requêtes à un serveur. Un serveur peut être spécialisé en serveur d'applications, de fichiers, de terminaux, ou encore de messagerie électronique.

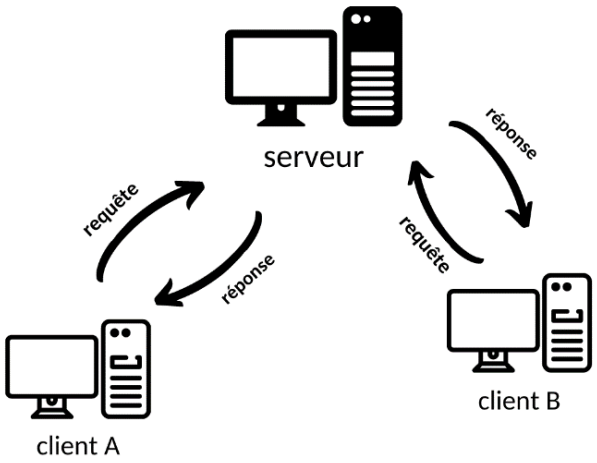

Figure 8 Architecture client/serveur.

a Client

Les caractéristiques d'un client sont les suivantes :

- Il envoie des requêtes au serveur
- Il attend et reçoit les réponses du serveur

b Un serveur

Les caractéristiques d'un serveur sont les suivantes :

- Il attend, il est à l'écoute.
- Prêt à répondre aux requêtes envoyées par des clients. Dès qu'une requête lui parvient, il la traite et envoie une réponse.

1.7 Outil de sécurité de réseaux informatiques

1.7.1 Pare-feu/firewall

Un système informatique pare-feu assure un contrôle d'accès strict entre vos systèmes et le monde extérieur.

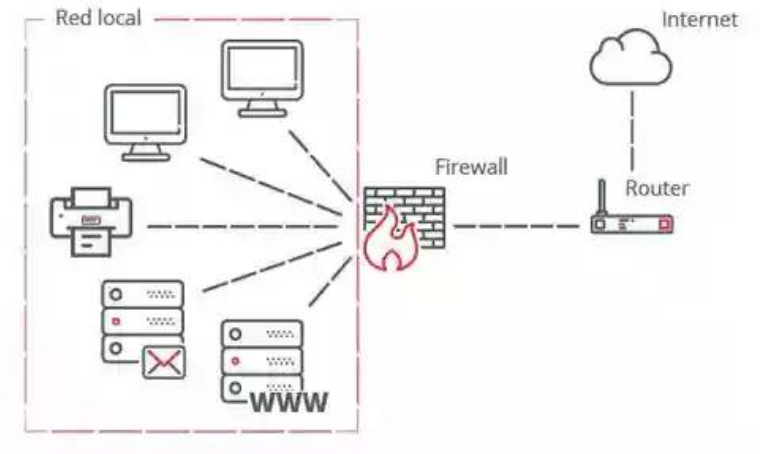

Figure 9: Diagramme Firewall. [11]

Le concept d'un pare-feu est un point de contrôle par lequel tout le trafic entre un réseau sécurisé et un réseau non sécurisé doit passer. En pratique, il s'agit généralement d'un point de contrôle entre un réseau d'entreprise et l'Internet. En créant un point unique par lequel tout le trafic doit passer, il est plus facile de surveiller et de contrôler le trafic et de concentrer l'expertise en matière de sécurité sur ce point unique. [12]

1.7.2 DMZ : Zone démilitarisée

Une DMZ est une méthode de mise en réseau qui sépare les serveurs auxquels on accède souvent de l'extérieur. Des services tels que les serveurs de messagerie et les serveurs http sont très souvent accessibles depuis l'extérieur, ce qui peut poser un risque de sécurité lorsque ces serveurs se trouvent sur le même réseau que vos serveurs contenant des données confidentielles.

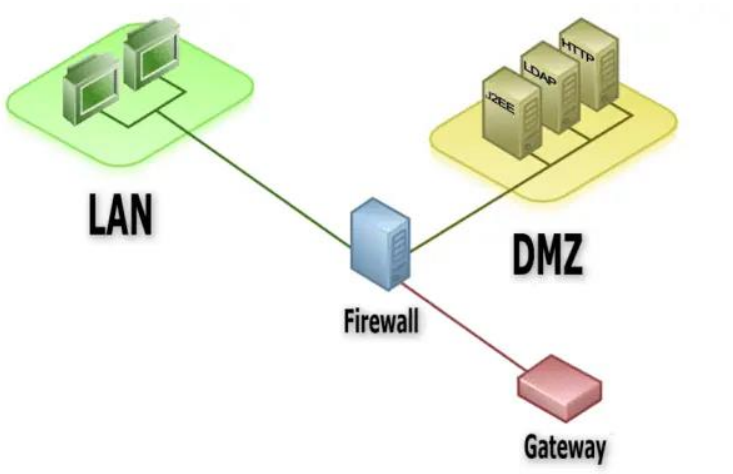

Figure 10: Diagramme DMZ. [13]

Certaines zones, telles que la chambre forte et les centres de contrôle, sont interdits à moins que vous ne soyez un membre du personnel autorisé. Les portes de ces zones sont souvent gardées selon des règles beaucoup plus strictes qu'à l'entrée. De même, le pare-feu permet à la majorité du trafic d'accéder aux services de la zone démilitarisée (DMZ) tout en appliquant des règles plus strictes lorsqu'il s'agit d'accéder aux serveurs internes. [14]

1.7.3 Proxy

Le serveur mandataire ou proxy est notamment utilisé pour le trafic du protocole de transfert de texte (HTTP) ou même du protocole de transfert de fichiers (FTP) entre le réseau local et l'Internet.

Interceptant une requête vers le monde extérieur, le proxy l'effectue en son nom propre, puis stocke les données renvoyées. Ensuite, il les retransmet au demandeur initial.

Le rôle du proxy est double. Premièrement, il permet de cacher les adresses IP internes, puisque la requête n'est pas étendue à l'Internet. Deuxièmement, il permet le filtrage, par exemple pour interdire l'accès à certains sites Web.

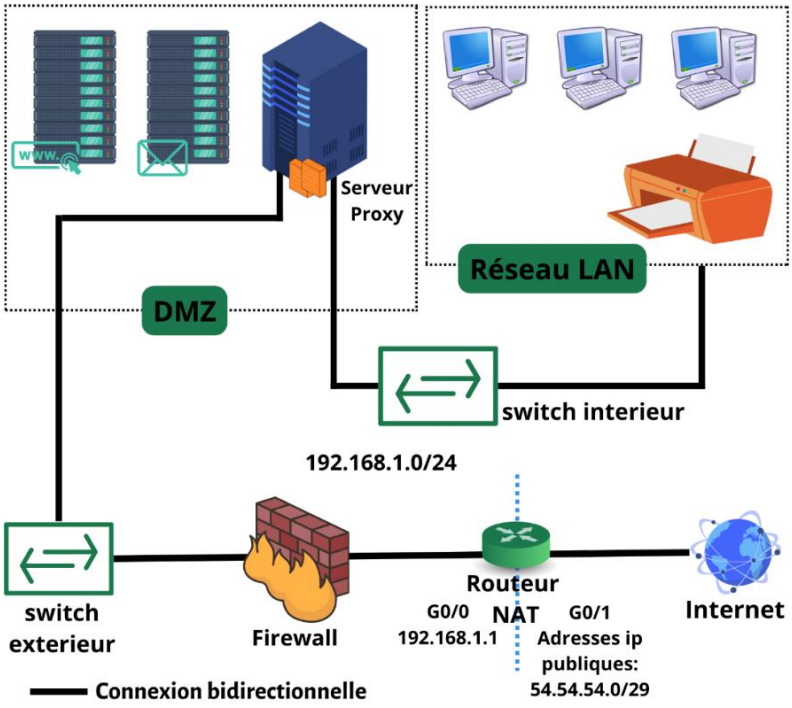

Figure 11: Architecture réseau d'une entreprise.

Un troisième avantage du proxy est sa capacité de gérer un cache. Ainsi, il est possible d'éviter de demander à nouveau un fichier ou un site sur Internet. En effet, un site dynamique change si régulièrement que l'on peut souvent considérer qu'il est rechargé à chaque requête. [15]

1.7.4 Le principe de fonctionnement de proxy :

Le serveur proxy doit se connecter au serveur auquel l'application souhaite se connecter, puis il envoie des requêtes au serveur, une fois que le proxy reçoit les réponses du serveur, elles sont envoyées au client de l'application et l'utilisateur se connecte enfin à la page web qu'il souhaite. [15]

1.8 Conclusion

Dans ce chapitre, nous avons étudié de manière générale les réseaux informatiques en mettant l'accent sur le protocole TCP/IP et ses principaux protocoles de communication ainsi que les différents outils de protection assurant leur sécurité.

Cette étude nous a permis d'approfondir nos connaissances dans le domaine des réseaux informatiques et plus précisément ceux des entreprises afin de nous permettre de bien mener le reste de notre travail.

Chapitre 2 Vie privée et anonymat sur internet

2.1 Introduction

L'anonymat sur Internet est de plus en plus requis, plusieurs personnes cherchent des moyens pour anonymiser leurs informations de navigation et de se protéger contre la surveillance illégale exercée par les gouvernements et les géants de l'informatique notamment les GAFAM (Google, Appel, Facebook, Amazon, Microsoft).

Les risques existent toujours à mesure que l'anonymat sur Internet devient plus fréquent. Pour mieux se protéger, il est important de savoir à quoi s'attendre, en procédant à l'étude détaillée de l'anonymat sur le Net, et les réseaux anonymes les plus courants.

Ce chapitre va porter sur les questions liées à la vie privée sur internet et les différents moyens permettant de garantir l'anonymat notamment l'utilisation des réseaux anonymes VPN, TOR, I2P, JONDONYM. Il traitera également des risques associés à l'utilisation de ces moyens qui permettent aux utilisateurs de contourner les mesures de protection établies et d'accéder au DarkWeb pour mener potentiellement des actions malveillantes.

2.2 La vie privée sur internet

Il s'agit généralement d'un échange libre de certains contenus que l'on souhaite garder pour soi, mais que l'on transmet à d'autres personnes de confiance et à personne d'autre au cours de la conversation. Il ne s'agit presque jamais d'une conversation secrète, dans laquelle l'environnement ne peut pas voir **qui** tient la conversation, le plus important est que le **contenu** de la conversation reste privé. [16]

2.3 L'anonymat sur internet

L'anonymat n'a pas la même signification que la vie privée, c'est surtout une préoccupation liée à "invisibilité" ou "introuvabilité" d'une ou plusieurs personnes dans leur environnement.

En effet, dès qu'un utilisateur se connecte à Internet, ses activités sont scrupuleusement analysées et retracées pour pouvoir l'identifier et le retrouver. Dans ce contexte, l'anonymat permet de communiquer un contenu, quel que soit son degré de confidentialité, au public le plus large possible, sans être en mesure de retracer la source de cette information.

L'anonymat est employé particulièrement par les lanceurs d'alertes (comme c'était le cas pour Edward Snawden pour dénoncer les programmes de surveillance de masse américain et britannique) qui, prenant conscience d'un danger, d'un risque ou d'un scandale, adresse un signal d'alarme en espérant enclencher un processus de régulation, de controverse ou de mobilisation collective sans pour autant déclarer leur identité. [16]

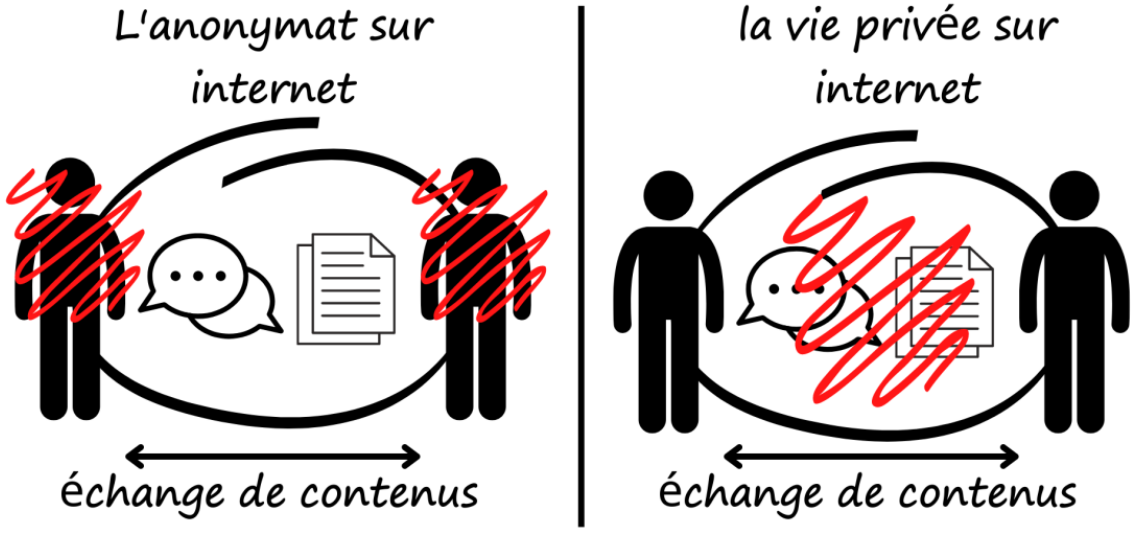

Figure 12: Différence entre vie privée et anonymat sur internet.

- l'anonymat est-il possible au XXIe siècle numérique ?

L'anonymat n'est pas quelque chose de nouveau sur Internet, plusieurs solutions ont été développées afin de permettre aux utilisateurs de communiquer de manière anonyme. Toutefois cet anonymat n'est jamais parfait, puisqu'il est toujours possible de

remonter à l'auteur, surtout si ce dernier utilise toujours le même moyen pour préserver son anonymat.

Dans le cas le plus simple d'anonymat, les utilisateurs emploient des faux profils ou des faux noms pour échanger des e-mails ou pour participer incognito à des forums de discussion dès lors que ces services ne vérifient par leur identité. Toutefois cette technique ne garantit pas l'anonymat étant donné que l'adresse IP de l'utilisateur est visible et peut être utilisée pour l'identifier.

Il existe également d'autres méthodes bien connues pour rendre l'anonymat, que nous aborderons plus en détail ultérieurement.

2.4 DeepWeb

Le DeepWeb représente la partie cachée du Web qui est constitué du contenu des bases de données et autres services du web qui, pour une raison ou une autre, ne sont pas indexés par les moteurs de recherche classique que tout le monde utilise. [18]

2.5 DarkWeb

Le DarkWeb fait référence à un contenu en ligne crypté qui n'est pas indexé par les moteurs de recherche conventionnels. L'accès au DarkWeb ne peut se faire qu'à l'aide de navigateurs spécifiques, tels que le navigateur JondoBrowser. L'utilisation de ce réseau est caractérisée par la confidentialité et l'anonymat des activités par rapport aux réseaux internet traditionnels. [17]

2.5.1 Différence entre DarkWeb et DeepWeb

Contrairement au DeepWeb, le DarkWeb est un énorme monde cyber clandestin où des personnes et des organismes malveillants tels que les pirates, les gangsters, les terroristes et les pédophiles y vont pour acheter ou vendre toute sorte de produits interdits. Véritable marché noir, ses marchandises et services ne sont pas payés par des moyens classiques tels que les cartes de crédit, puisqu'elles permettent de remonter au fournisseur et au client mais plutôt par les cryptos-monnaies. [18]

2.5.2 Accès au DarkNet

Pour accéder au Darknet, procédez comme suit :

1. Installez JonDo le changeur d'IP qui est un programme proxy gratuit et open source écrit en Java qui vous connectera au réseau JonDonym pour assurer l'anonymat de votre identité.
2. Installer JonDoBROWSER le navigateur du réseau JonDonym.
3. Une fois JonDo téléchargé et installé sur votre appareil et le navigateur JonDoBROWSER prêt, il vous faudra aller chercher des liens dans le Darknet.

Pour cela, il faut aller sur ce qu'on appelle un annuaire de liens du Darknet. Il en existe beaucoup, mais l'un des plus célèbres est "inthehiddenwiki.net". Tapez cela dans la barre de recherche pour être redirigé vers une page qui ressemble beaucoup à Wikipedia... mais avec un contenu un peu différent. Vous devrez ensuite passer un certain temps à chercher dans le Darknet pour trouver des sites qui vous semblent pertinents.

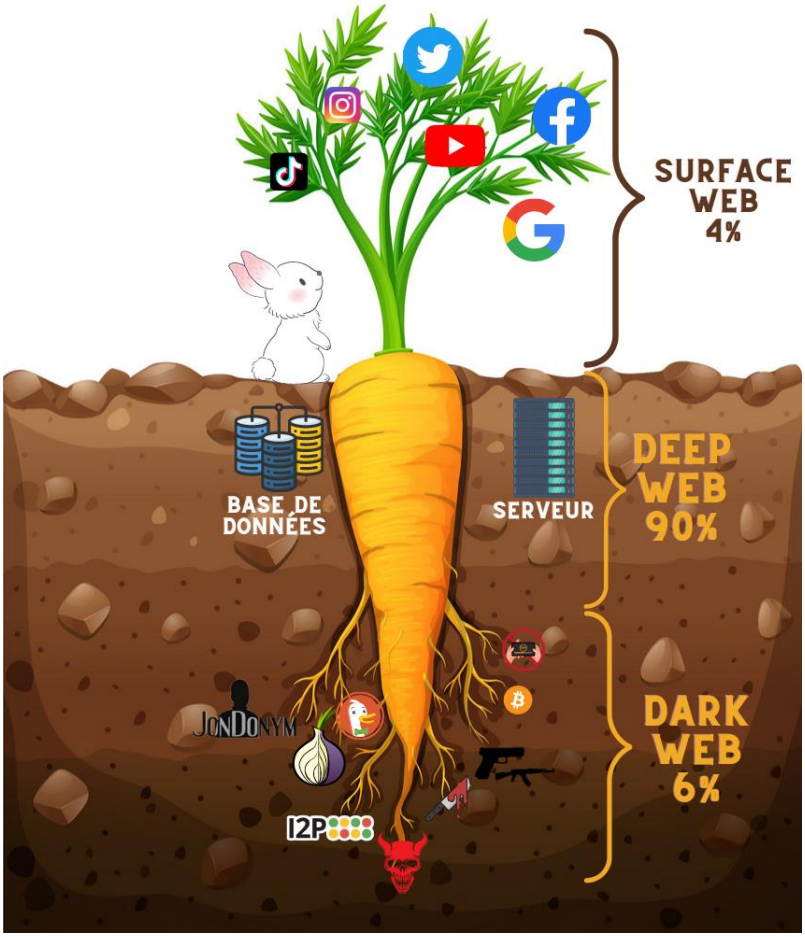

Figure 13: Différence entre le darkweb et le Deepweb.

2.6 Les outils d'anonymat

2.6.1 Réseau TOR

TOR est l'acronyme de « THE ONION ROTING ». Il s'agit d'un logiciel qui permet de brouiller l'empreinte digitale laissée par les utilisateurs au cours de leur utilisation du réseau Internet en les rendant virtuellement introuvable. [19]

a Principe de fonctionnement

Le TOR est un réseau informatique qui garantit l'anonymat de ses utilisateurs grâce à un chiffrement multicouche appelé aussi routage onion. Le trafic des utilisateurs transite par plusieurs relais (ordinateur des participants), et est chiffré à chaque étape. Le principe de fonctionnement est le suivant : le proxy TOR calcule un itinéraire, récupère les clés publiques des nœuds associés, et chiffre les données avec ces clés publiques, tour à tour.

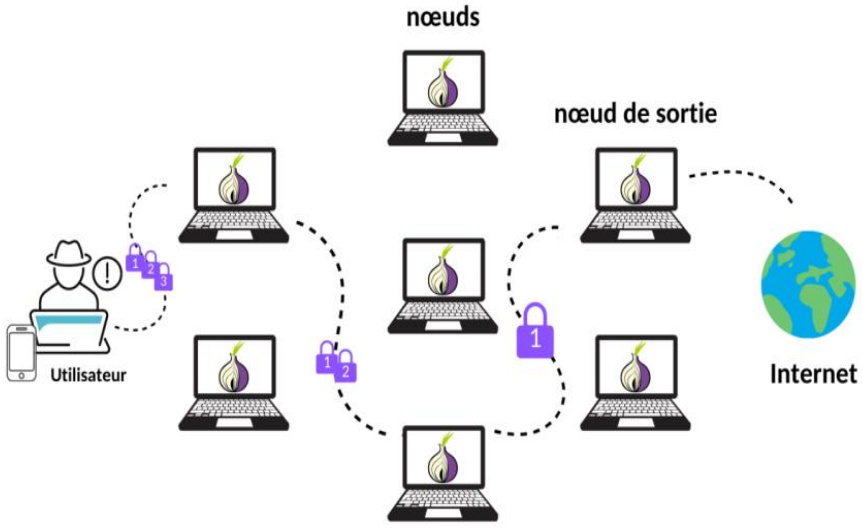

Figure 14 Le principe de fonctionnement du réseau TOR

Les données sont chiffrées entre l'ordinateur source et le nœud d'entrée, qui déchiffre « sa partie » et transmet au suivant, qui fait de même, et ainsi de suite. Le paquet chiffré perd une « couche » de chiffrement à chaque saut, jusqu'au moment où il va atteindre le nœud de sortie : ce dernier va faire sauter la dernière couche de chiffrement, et transmettre le paquet en clair à son destinataire final.

Par défaut, Tor anonymise uniquement la navigation sur le Web, mais vous pouvez le configurer pour qu'il fonctionne avec un logiciel tiers afin d'anonymiser d'autres activités Web, telles que l'envoi d'e-mails. [19]

b Avantages et inconvénients

Tableau 3: Avantages et inconvénients du réseau TOR.

Les avantages	Les Inconvénients
• Personne ne peut tracer les sites que vous visitez. • Le trafic des utilisateurs est soumis à un triple chiffrement, très difficile à intercepter.	• Très lent car les données sont acheminées via une série de relais. • Certains FAI recherchent et bloquent activement les relais Tor, ce qui rend difficile la connexion de certains utilisateurs. • Le Tor est un programme libre son code source est accessible à tous ceux qui souhaitent le voir

2.6.2 Réseau I2P

I2P signifier « le projet internet invisible » dont l'objectif principal est de construire, déployer, et maintenir un réseau fournissant des communications sécurisées et anonyme.

Dans I2P, les utilisateurs peuvent contrôler le niveau de sécurité de l'anonymat et la bande passante qui répond à leur besoin spécifique. L'anonymat d'I2P est assuré du fait que l'expéditeur et le destinataire ne communiquent jamais directement mais passent par plusieurs routeurs appelées tunnels. [20]

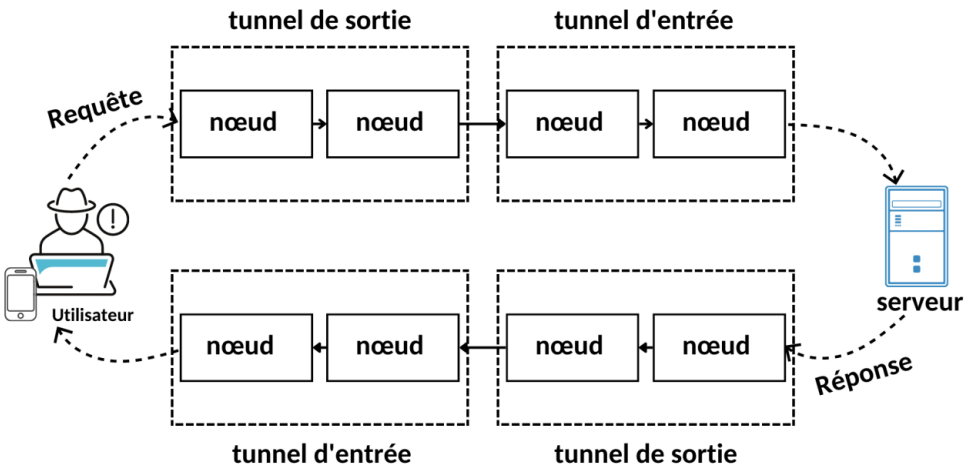

Figure 15 Le principe de fonctionnement du réseau I2P.

a Principe de fonctionnement

Le fonctionnement d'I2P est similaire au fonctionnement d'autres réseaux anonymes, où le trafic est acheminé à travers différents points du réseau à l'aide de chaines de serveur proxy.

I2P est un réseau dans le réseau, c'est-à-dire que tous les ordinateurs constituant ce réseau sont connectés entre eux et sont totalement isolés du reste de l'internet autrement dit, toutes les connexions passent par des tunnels chiffrés. Les adresses IP ne sont pas utilisées et sont remplacés par des clés asymétriques. Tout ordinateur connecté à I2P est considéré comme un serveur internet, il synchronise un carnet d'adresse ou se trouvent les autres sites qui s'appellent des eps sites. Bien qu'il présente des similitudes avec d'autres réseaux anonymes, I2P ne cherche pas à améliorer l'anonymat de ses participants. Il s'agit d'un réseau orienté message ou chaque paquet de données est acheminé de manière anonyme vers sa destination correspondante. Cela signifie que lorsqu'un expéditeur envoie un message les autres participants au réseau peuvent connaitre l'existence d'utilisateur. [20]

b Avantages et inconvénients

Tableau 4: Avantages et inconvénients du réseau I2P.

Les avantages	Les Inconvénients
• Effectuer une analyse du trafic très difficile. • Il est compatible avec les navigateurs les plus importants. • Peut être utilisé dans toutes les activités effectuées sur le Web.	• Ne garantit pas un anonymat parfait lors de l'utilisation du Web de surface pour visiter des sites indexés. • Le processus d'installation et les paramètres du navigateur sont complexes.

2.6.3 Définition de VPN :

Les réseaux privés virtuels, souvent appelés VPN pour Virtual Privat Network, offrent à un client VPN une extension du réseau privé de l'entreprise à travers un support public comme internet.

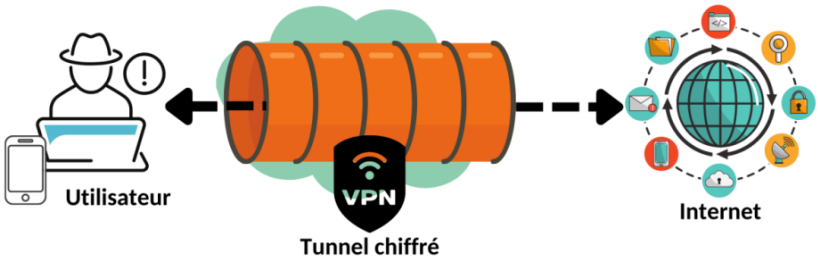

Figure 16 Le principe de fonctionnement du VPN.

Après activation du VPN, un tunnel sécurisé est créé entre vous et le réseau internet. Par conséquent, les informations qui y transitent seront cryptées et que l'activation se fait en se connectant à un serveur VPN distant. Ainsi, vous obtiendrez une nouvelle adresse IP usurpée et votre adresse IP sera bloquée. [19]

a Principe de fonctionnement

L'utilisateur se connecte au fournisseur VPN à travers une connexion Internet. Ce dernier crypte toutes les informations stockées ou envoyées sur le réseau. Les connexions VPN permettent également aux internautes d'accéder à du contenu qui ne serait autrement pas accessible à leur emplacement. Les connexions VPN aident les utilisateurs à masquer leurs adresses IP. [19]

b Avantages et inconvénients

Tableau 5: Avantages et inconvénients du VPN.

Les avantages	Les Inconvénients
• Maintient l'anonymat sur Internet. • Protège contre toute forme de surveillance et d'espionnage en ligne.	• Ralentie la connexion internet et la rend instable. • Sous-traiter ses données à un acteur externe inconnu.

2.7 Le réseau JonDonym

Le réseau JonDonym est un système de proxy conçu qui vous permet de naviguer sur Internet à l'aide de pseudonymat révocable (utilisé ou posté avec des pseudonymes,

des noms fictifs). Sans cet anonymat, tous les appareils qui utilisent Internet utiliseront des adresses traçables.

Les fournisseurs d'accès ainsi que des tiers tracent et collectent des informations sur les utilisateurs notamment les sites qui sont allés visiter et leurs données personnelles dans le but de les surveiller ou d'influencer leur décision par le contrôle du contenu qui leur sera proposé dans les différents services qu'ils utilisent. Cette surveillance est d'autant plus facile si ces utilisateurs n'utilisent pas des connexions cryptées.

. Cependant, le JAP empêche les tiers et les sites visités de collecter des informations sur les utilisateurs en utilisant une adresse statique partagée par d'autres utilisateurs JAP. [21]

- **JonDonym** est une branche de développement du projet AN.ON.
- **JAP** est le prédécesseur de JonDo, le logiciel client qui connecte les utilisateurs au réseau de mix JonDonym/AN.ON.
- **JonDos** est la société qui développe activement JonDo et est l'instance de facturation entre les utilisateurs et les opérateurs de mix.
- **JonDonauts** sont ceux qui surfent anonymement via le réseau JonDonym.

2.7.1 Historique

JonDonym est le système d'anonymisation d'Internet, bien connu en Allemagne. Il s'agit également du produit principal de la société JonDos, fondée en 2007 à la suite d'un projet de recherche universitaire. Entre-temps, JonDos offre des services informatiques dans divers domaines du développement de logiciels généraux et de l'intégration de logiciels. [22]

2.7.2 MIX network

Un réseau mixte assure l'anonymat en relayant les messages par un chemin de nœuds mix (ou mixes) d'une manière tolérante à la latence (retard). L'utilisateur crypte un message qui sera partiellement décrypté par chaque mix le long du chemin.

Les mixes acceptent un lot de messages cryptés, qui sont partiellement décryptés, permutés de manière aléatoire et transmis. Un observateur est incapable de corréler les

messages entrants et sortants au niveau du nœud de mélange ; ainsi, les réseaux de mélange offrent l'anonymat contre un puissant adversaire passif global. En fait, tant qu'un seul nœud de mélange sur le chemin de l'utilisateur n'est pas compromis, le message conserve un certain anonymat.

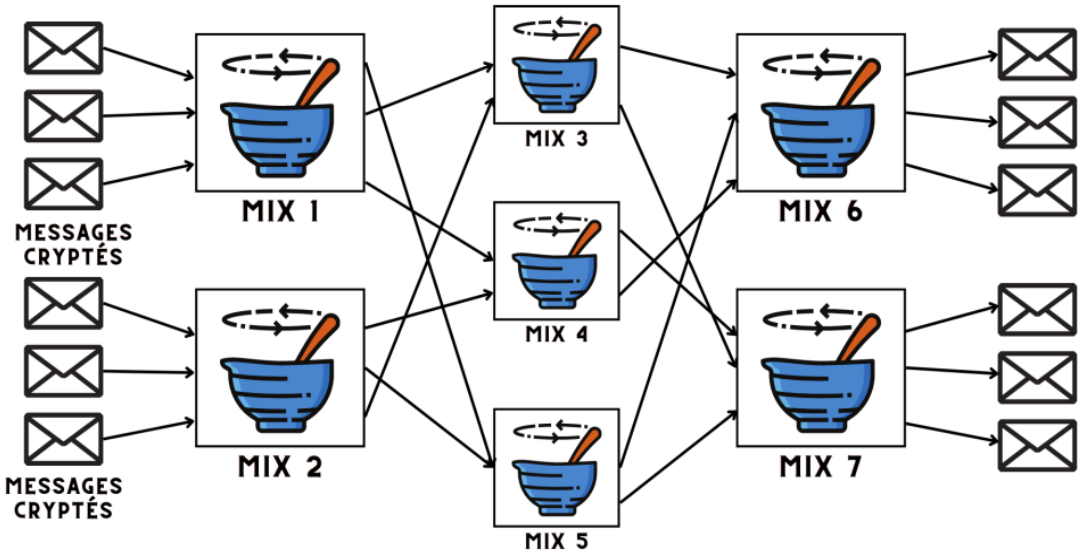

Figure 17: Mixnet avec topologie en couches (3 couches de Mixes).

Cependant, le regroupement des messages au niveau d'un nœud de mélange introduit des retards inhérents, ce qui rend les réseaux de mélange inadaptés aux applications interactives à faible latence (par exemple, la navigation sur le web, la messagerie instantanée). Lorsqu'ils sont utilisés, c'est pour des applications tolérant la latence, comme le courrier électronique anonyme. [23]

2.7.3 Fonctionnement du Java Anon proxy (JAP)

Lorsque JonDonym est utilisé, l'utilisateur n'est pas directement connecté au site demandé. Au lieu de cela, l'utilisateur emprunte un long chemin pour se connecter au site. Le long chemin consiste en une connexion avec cryptage via différents intermédiaires, connus sous le nom de Mixes. [21]

Le proxy local (JAP) et les serveurs de Mix communiquent à travers des connexions Internet TCP/IP. Chaque JAP a une seule connexion à un serveur de Mix. Un serveur de Mix à une seule connexion à un ou deux autres Mixes. Si un Mix reçoit des paquets de données

de JAP's et les envoie à un autre Mix, nous l'appelons un premier Mix. Un premier Mix a donc exactement une connexion à un autre Mix. Si un Mix reçoit des paquets d'un Mix et envoie les données au proxy de cache, nous l'appelons le dernier Mix. Par conséquent, un dernier Mix n'a qu'une seule connexion à un autre Mix. Chaque Mix ayant deux connexions à d'autres Mix est appelé Mix intermédiaire. Ce type de Mix recevra des paquets d'un Mix et les transmettra à l'autre Mix.

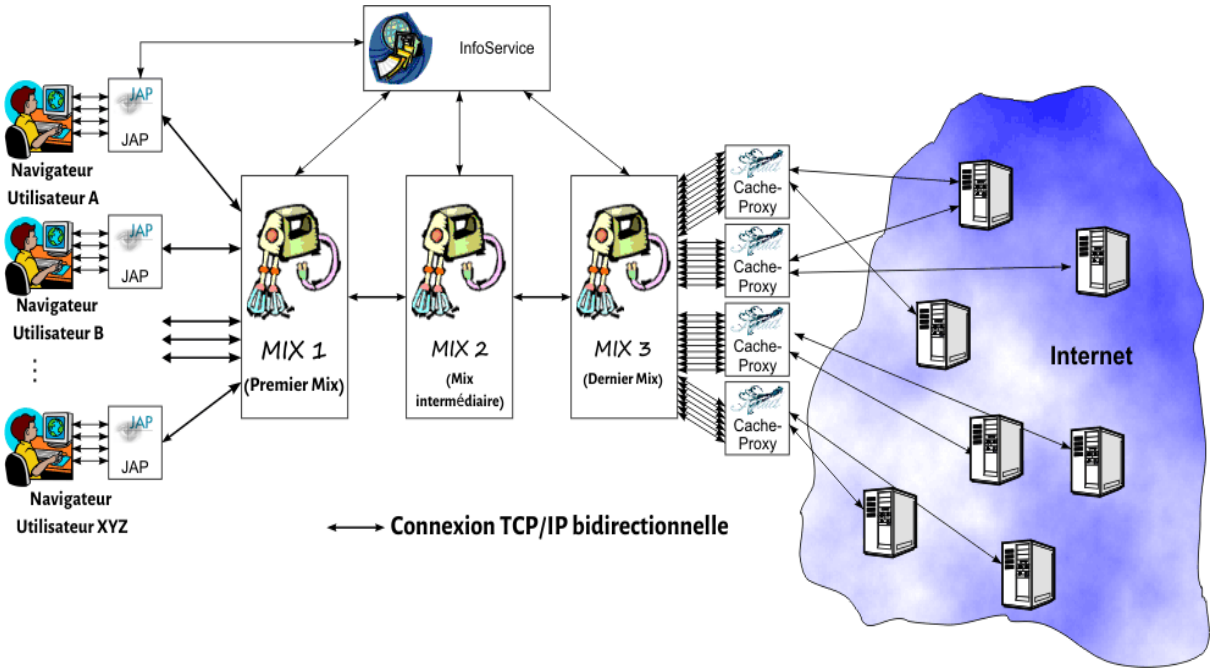

Figure 18: Fonctionnement de JAP. [**24**]

Si les Mixes sont connectés de manière significative, une chaîne est mise en place, de sorte que les paquets sont transmis des JAP aux cache-proxies, puis à Internet. Une chaîne de Mixes est appelée une MixCascade. Plusieurs cascades différentes peuvent exister en même temps, mais le JAP peut en sélectionner une seule à la fois.

De même, un Mix ne peut faire partie que d'une seule et unique cascade. Si un Mix ne fait pas partie d'une cascade, nous l'appelons un Mix libre. Les Mix libres ne sont pas utilisables pour les JAP, mais peuvent être connectés pour construire une nouvelle cascade.

En plus des JAPs et des Mixes, un troisième composant est ajouté au système : l'InfoService. L'InfoService est plus ou moins une base de données qui stocke des informations sur le système, comme les MixCascades disponibles, le statut des Mixes, etc. [24]

2.7.4 Mulitplexage et démultiplexage

Le JAP agit comme un proxy local pour le navigateur. Le navigateur ouvre de nombreuses connexions au JAP (généralement une par requête HTTP). Toutes ces connexions sont multiplexées sur une seule connexion au premier mix auquel JAP est connecté.

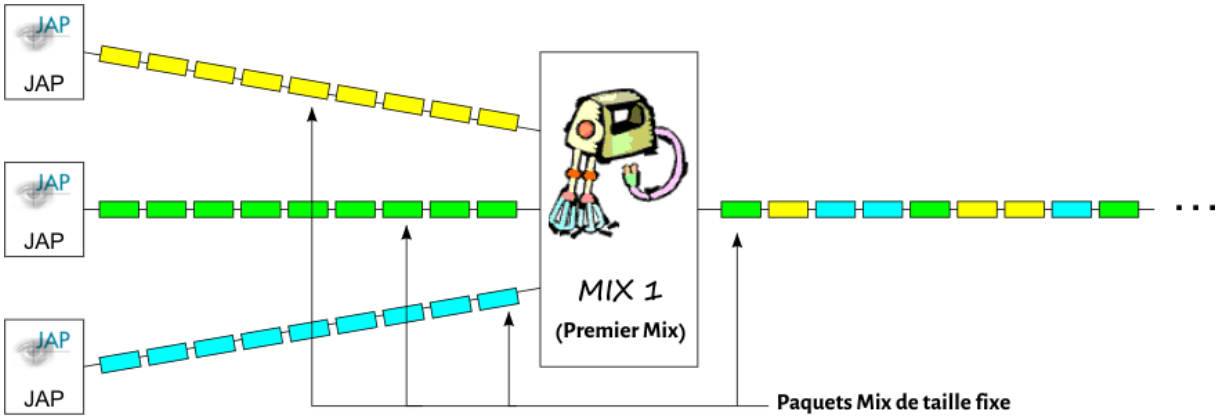

Figure 19: Mulitplexage et démultiplexage de MixPackets de taille fixe. [**24**]

Chaque connexion du navigateur est appelée un canal (canal de mixage ou AnonChannel). Un premier mix envoie le flux de paquets (plusieurs canaux) de plusieurs utilisateurs au mix suivant (le tout sur une connexion TCP/IP). JAP et les mixes doivent donc multiplexer/démultiplexer les canaux. Un canal ne peut transporter que des paquets de taille fixe. Ces paquets sont appelés MixPackets. Ainsi, un premier mix par exemple reçoit de nombreux paquets de différents utilisateurs en parallèle et les envoie au mix suivant de manière sérialisée. [24]

2.7.5 Cryptage dans Java Anon Proxy (JAP)

Le cryptage des données est d'abord effectué par le logiciel JonDonym. Les données cryptées sont ensuite envoyées à la première station de mixage, cette dernière mélange les données cryptées avec les données d'autres utilisateurs, puis les données sont reçues par la seconde station de mixage.

La deuxième station de mixage transfère ensuite les données vers le troisième mixage où le décryptage se produit, puis les données sont envoyées sur Internet via la cache proxy.

Une couche de cryptage entoure les données du dernier mixage de la cascade de mix. Seul le dernier mix peut supprimer cette couche pour récupérer les données. Une autre couche de cryptage est placée autour des données déjà cryptées pour l'avant-dernier mix, de la même manière, la troisième couche de cryptage se produit du troisième au dernier mélange. [21]

2.7.6 Types de cryptages dans Java Anon Proxy

Java Anon Proxy utilise le processus cryptographique asymétrique pour effectuer le cryptage afin que chaque couche de cryptage ne soit supprimée que par le mélange approprié.

Les processus cryptographiques asymétriques sont différenciés par leur utilisation des deux clés : une clé secrète qui est utilisée pour décrypter les données cryptées, et l'autre est la clé publiquement connue qui est utilisée pour effectuer le cryptage des données.

La clé secrète est connue uniquement par la station de Mix spécifique par laquelle les données chiffrées sont censées être déchiffrées. Voici les deux méthodes de chiffrement utilisées par le proxy Java Anon. [21]

- AES avec la longueur de clé de 128 bits sachant qu'AES est un algorithme de chiffrement/déchiffrement symétrique.

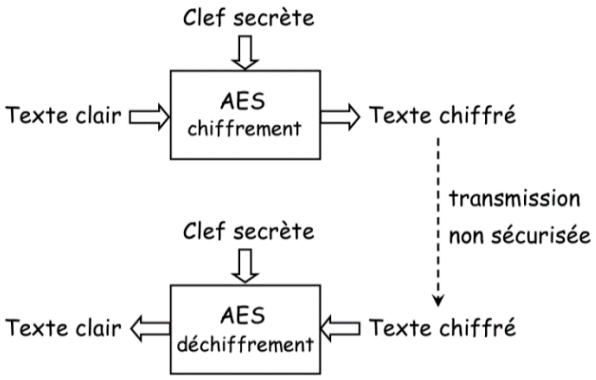

Figure 20: Chiffrement AES. [**25**]

Une même clef secrète est utilisée pour les opérations de chiffrement et de déchiffrement (c'est un secret partagé entre l'expéditeur et le destinataire du message). AES est un algorithme de chiffrement par blocs, les données sont traitées par blocs de 128

bits pour le texte clair et le chiffré. La clef secrète a une longueur de 128 bits, d'où le nom de version : AES 128 (il existe deux autres variantes dont la clef fait respectivement 192 et 256 bits). [25]

- RSA avec la longueur de clé de 1024 bits est asymétrique : il utilise une paire de clés (des nombres entiers) composée d'une clé publique pour chiffrer et d'une clé privée pour déchiffrer des données confidentielles.

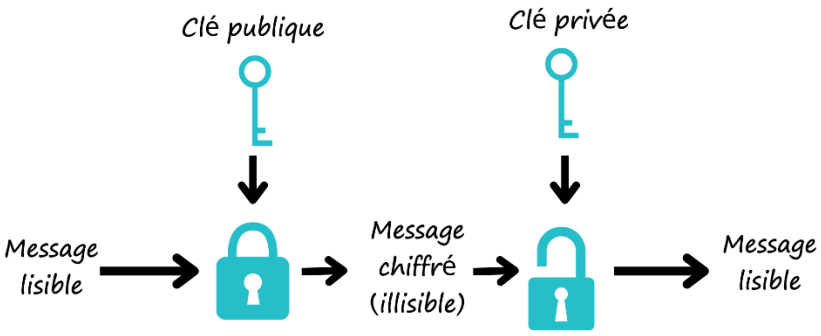

Figure 21: Chiffrement RSA.

L'algorithme RSA est un algorithme de cryptographie asymétrique. Asymétrique, signifies en fait qu'il fonctionne sur deux clés différentes, à savoir la clé publique et la clé privée. Comme son nom l'indique, la clé publique est donnée à tout le monde et la clé privée est gardée privée.

Un client envoie sa clé publique au serveur et demande certaines données.

Le serveur crypte les données en utilisant la clé publique du client et envoie les données cryptées.

Le client reçoit ces données et les décrypte. [26]

Pour avoir une plus grande efficacité, les données sont chiffrées symétriquement avec l'AES. La méthode RSA asymétrique plut lente effectue le chiffrement de la clé symétrique.

a Établissement d'un AnonChannel

Avant de pouvoir envoyer des données via un canal Anon, il faut en établir un. Ceci est fait en envoyant des messages d'ouverture de canal à travers les mixes. La figure 22 montre le format d'un tel message, comment il arriverait par exemple au dernier mix.

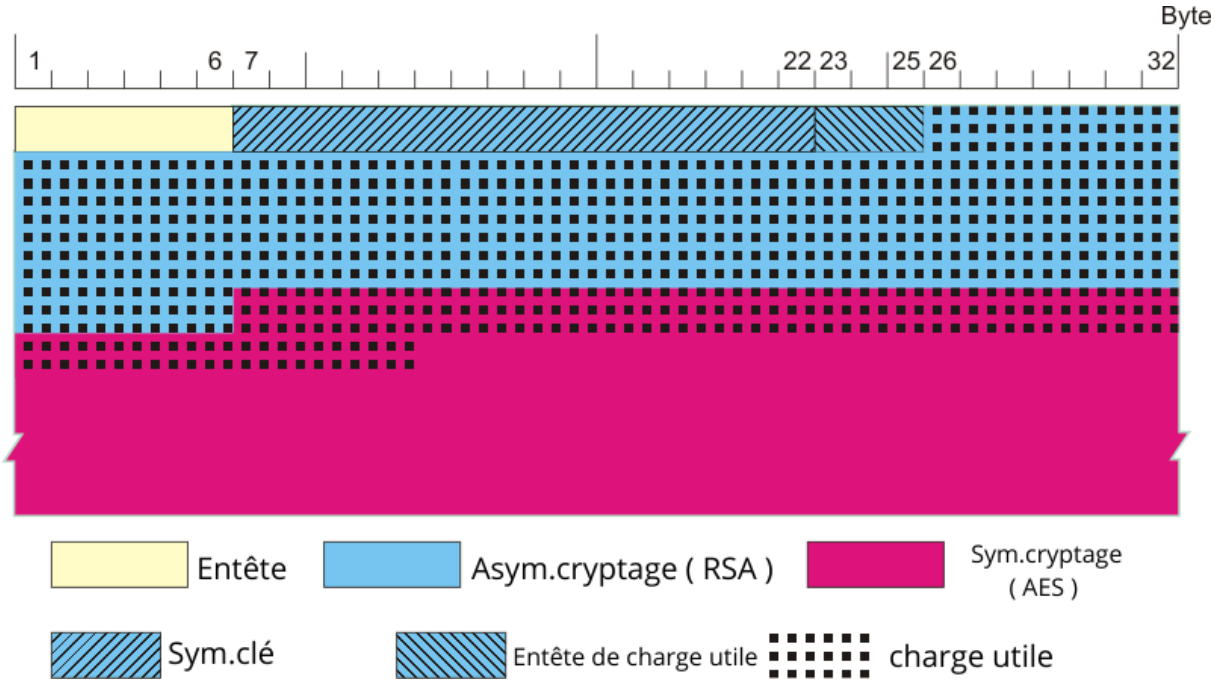

Figure 22: Paquet ChannelOpen (exemple pour le dernier Mix). [**24**]

b Avantages du chiffrement

Il y a deux raisons principales pour lesquelles le cryptage est si important pour atteindre l'anonymat.

1. Pour s'assurer que les données cryptées sont correctement décryptées par le mélangeur réel, et non par un espion ou un attaquant. [19]
2. Différents niveaux de cryptage rendent vos données plus sûres, car elles ont un aspect différent à chaque fois qu'elles sont cryptées. Cela rend très difficile pour un attaquant de connecter un message sortant à un message entrant en fonction de l'apparence des données. [19]

c Avantages et inconvénients du réseau JONDONYM

Tableau 6: Avantages et inconvénients du réseau JONDONYM.

Les avantages	Les Inconvénients
• Il empêche la fuite d'informations supplémentaires pendant l'utilisation de l'anonymiseur. • Les utilisateurs peuvent choisir eux-mêmes à qui de ces opérateurs ils feront confiance et à qui ils ne feront pas confiance.	• Jondo est encore plus lent Par rapport au d'autres réseaux anonymes. • La sélection des nœuds est moins aléatoire, les journaux de jondo sont plus faciles à collecter.

2.7.7 Les risque d'utilisation les réseaux anonymes

Les réseaux anonymes tels que TOR, I2P et JONDONYM garantissent la confidentialité. Cependant, l'utilisation de réseaux anonymes est souvent associée au DarkWeb, que les cybercriminels utilisent pour naviguer sur le côté obscur d'Internet et mener des activités illégales.

Les internautes peuvent utiliser le DarkWeb pour louer divers services criminels. Qu'il s'agisse de drogues, d'argent ou même de trafic d'êtres humains, le darkweb offre une plateforme pour toutes sortes d'infractions. Voici quelques exemples de crimes DarkWeb

- **Louer pour assassiner :** Le site Besa Mafia (et d'autres semblables) est un marché pour les meurtres de contrat.
- **Chantage/extorsion :** Une escroquerie qui consiste à menacer une victime de divulguer ses informations sensibles ou des photos compromettantes, à moins qu'elle ne paie une quantité déclarée de Bitcoin.
- **Ventes de drogues illicites :** AlphaBay était la plus grande source de fentanyl et d'héroïne sur le DarkWeb. Le ministère de la Justice l'a fermée en 2017. Des centaines de milliers de personnes l'ont utilisé pour acheter des pièces d'identité

frauduleuses, des produits contrefaits, des logiciels malveillants, des armes à feu et des produits chimiques toxiques.

- **Ventes d'armes illégales :** des dizaines de milliers de dollars sont utilisés chaque mois pour financer illégalement des contrats d'achat d'armes à travers le DarkWeb selon les estimations. [27]

2.8 Méthode d'analyse des paquets (DPI)

L'inspection approfondie des paquets est la collecte, la surveillance, l'analyse et/ou le stockage des données liées aux applications présentes dans les paquets Internet au-dessus de la couche 3 de l'OSI.

Le DPI est un type de technologie basé sur la détection des champs de caractéristiques. En lisant en profondeur le contenu de la charge de paquets IP et en réorganisant les informations de la couche application, on obtient le contenu de toute la couche application, le contenu du flux de données est analysé et détecté.

L'inspection approfondie des paquets nécessite que l'équipement soit capable d'analyser, de détecter et de réorganiser rapidement les données d'application pour éviter un retard excessif de l'application. [28]

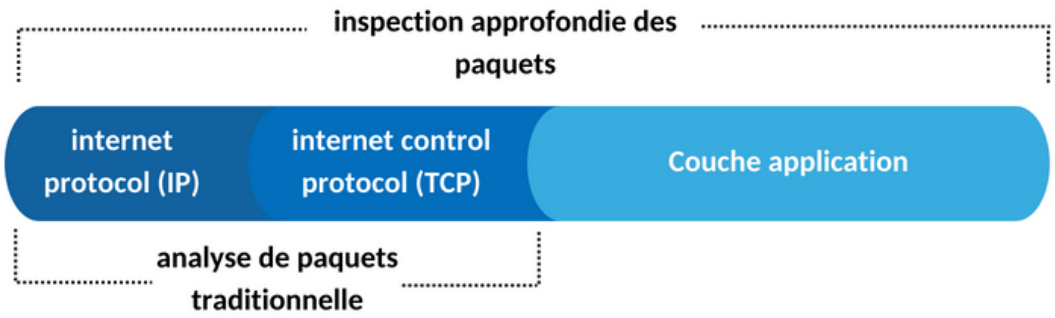

Figure 23 Deep Packet Inspection.

La plupart du matériel de DPI axé sur la couche réseau cible l'inspection des paquets IP. Les paquets IP contiennent toutes les informations pertinentes nécessaires au routage. Il s'agit donc d'une cible obligatoire lorsqu'on cherche à révéler l'identité des utilisateurs. L'analyse est effectuée principalement sur l'en-tête IP ; plus précisément, sur l'adresse source, l'adresse de destination et le type de protocole. Ces données peuvent être utilisées

à différentes fins malveillantes ; l'analyse et le traitement des en-têtes IP peuvent conduire à l'identification directe de l'utilisateur impliqué dans la communication. [29]

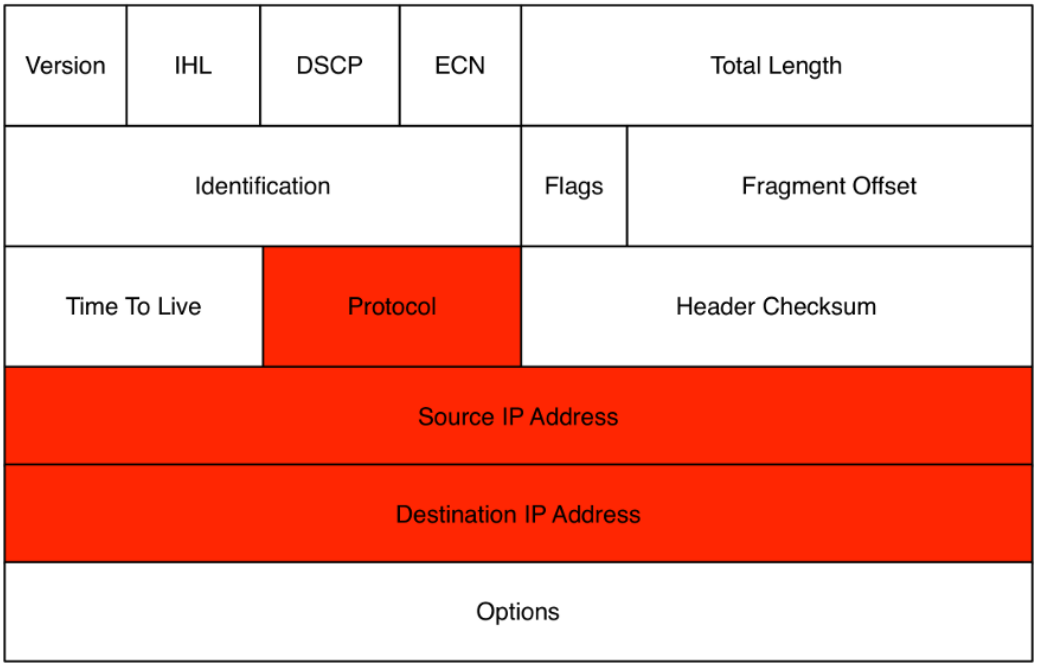

Figure 24: Champs de l'en-tête IPv4 couramment visés (rouge). [29]

2.8.1 Fonctionnement de l'inspection approfondie des paquets

L'inspection approfondie des paquets examine le contenu des paquets passant par un point de contrôle donné, et prend des décisions en temps réel en fonction de ce qu'un paquet contient et en fonction des règles attribuées par une entreprise, un fournisseur de services Internet ou un gestionnaire de réseau.

Les formes précédentes de filtrage de paquets ne regardaient que les informations d'en-tête de paquet, ce qui revient à lire une adresse imprimée sur une enveloppe sans aucune connaissance du contenu de l'enveloppe, cela était dû en partie aux limites de la technologie plus ancienne.

Jusqu'à récemment, les pare-feu n'avaient pas la puissance de traitement nécessaire pour effectuer des inspections plus approfondies sur de gros volumes de trafic en temps réel. Les progrès technologiques ont permis à DPI d'effectuer des inspections plus avancées afin de pouvoir vérifier à la fois les en-têtes de paquets et les données. [28]

2.8.2 L'analyseur de paquets Wireshark

C'est un logiciel Open source, permettant de comprendre les données que vous capturez à partir d'un réseau. Les données capturées sont interprétées et présentées sous forme de paquets individuels pour analyser le tout. Wireshark est utilisé dans le dépannage et l'analyse de réseaux informatiques, le développement de protocoles, l'éducation, mais aussi le piratage. Wireshark reconnaît actuellement 759 protocoles différents. [30]

a Principe de fonctionnement de wireshark

Wireshark collecte le trafic réseau via l'interface réseau de l'ordinateur, en mode discret (si nécessaire), pour inspecter et afficher des informations sur les protocoles, les adresses IP, les ports, les en-têtes et la longueur des paquets. [30]

Vous devez disposer des privilèges nécessaires pour exécuter Wireshark, il y a trois Processus suivis par chaque analyseur de paquets : collecte, conversion et analyse, sont décrits comme suit :

- **Collecter :** choisissez une interface pour écouter le trafic et capturer les paquets réseau.
- **Convertir :** augmenter la lisibilité des données non-lisibles par l'homme. Les paquets sont convertis en informations facilement compréhensibles via une interface graphique.
- **Analyser :** analysez le trafic réseau concernant les paquets, les protocoles, les données chiffrées et plus encore grâce à l'utilisation de fonctionnalités statistiques et graphiques.

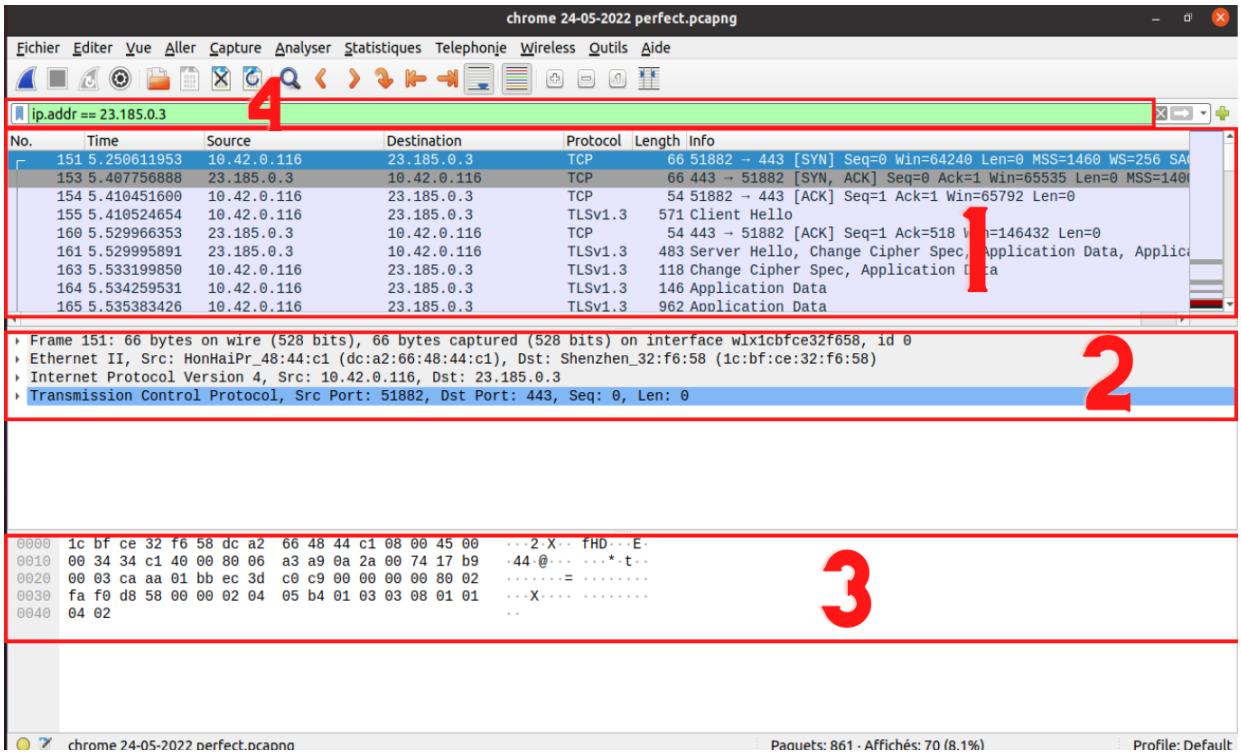

Figure 25: Fenêtre principale de l'interface de Wireshark.

- Section 1 sur la figure : affiche la liste des paquets capturés.
- Section 2 sur la figure : affiche les détails sur le paquet sélectionné de la liste du haut.
- Section 3 sur la figure : reproduit le contenu en hexadécimal, du même paquet.
- Section 4 sur la figure : applique un filtre d'affichage.

2.9 System de détection d'intrusion IDS

Un système de détection d'intrusions (Intrusion Detection System ou IDS) est un équipement matériel ou logiciel qui alerte l'administrateur en cas de faille de sécurité, de violation de règles ou d'autres problèmes susceptibles de compromettre son réseau informatique.

Certains termes sont souvent employés quand on parle d'IDS :

- Faux positif : une alerte provenant d'un IDS, mais qui ne correspond pas à une attaque réelle.
- Faux négatif : une intrusion réelle qui n'a pas été détectée par l'IDS.

Dans la section suivante, nous nous concentrons sur les fonctionnalités IDS de base concernant la source des données d'événement, l'approche de détection et l'emplacement de la collecte et du traitement des données. [31]

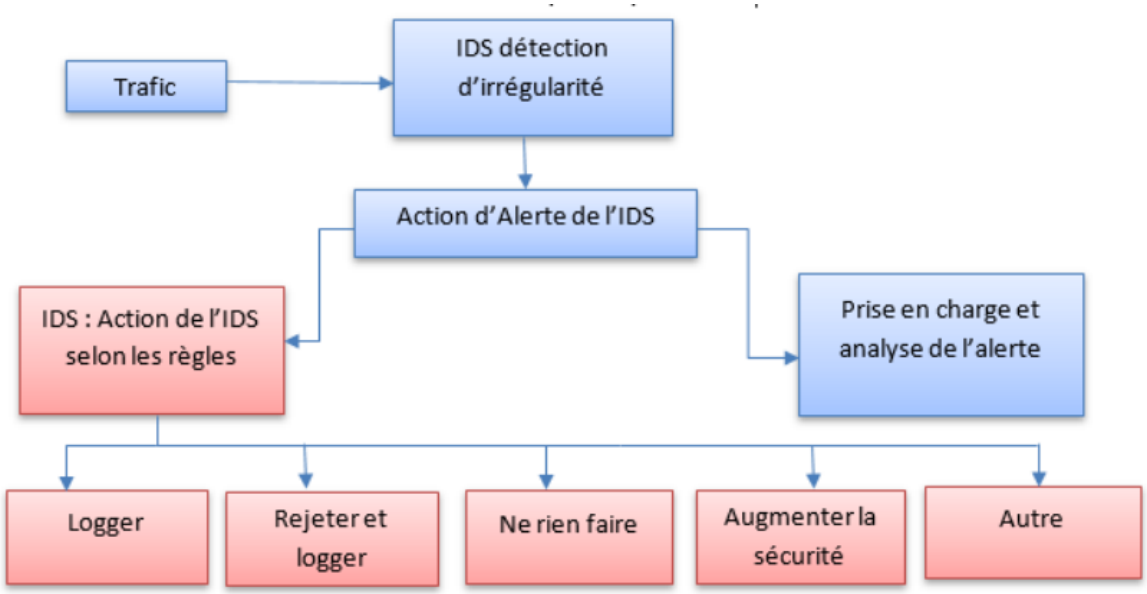

Figure 26: Le fonctionnement d'un IDS. [32]

Il existe deux catégories principales d'IDS.

- Les IDS basés sur le réseau (NIDS), qui lisent généralement les données d'événement directement à partir d'un réseau multidiffusion telle qu'Ethernet.
- Les IDS basés sur l'hôte (HIDS), qui collecte et analyse les données d'événement collectées sur l'hôte.

La méthode ou la technique de détection : deux catégories peuvent être distinguées

- Basée sur le comportement (également appelé détection d'anomalies).
- Basée sur les connaissances (à savoir la détection basée sur la signature ou la détection d'abus).

a Network Intrusion Detection System (NIDS)

Un IDS basé sur le réseau est un appareil qui surveille l'ensemble du trafic qui passe sur le segment de réseau ou qui surveille uniquement le trafic dirigé vers ou depuis l'hôte sur lequel il est installé. Ce type d'IDS présente l'avantage qu'un seul capteur, correctement placé, peut détecter des attaques qui visent plusieurs hôtes.

Les IDS basés sur le réseau sont souvent organisés comme un ensemble de capteurs ou d'hôtes à usage unique placés en divers points du réseau. Ces unités surveillent le trafic réseau, effectuent une analyse locale de ce trafic et signalent les attaques à une console de gestion centrale. [33]

b Host-based intrusion detection system (HIDS)

Un système de détection des intrusions basé sur l'hôte surveille l'hôte sur lequel le capteur est installé. Le flux d'événements peut être constitué de séquences d'appels système, d'enregistrements de journaux d'un ou plusieurs services, de journaux du système d'exploitation ou de tout autre journal d'activités au sein de la machine surveillée.

Lavantage de HIDS est qu'il ne nécessite pas de matériel supplémentaire. Cependant, il peut entraîner une dégradation significative des performances de son hôte en raison de la surcharge des opérations. [33]

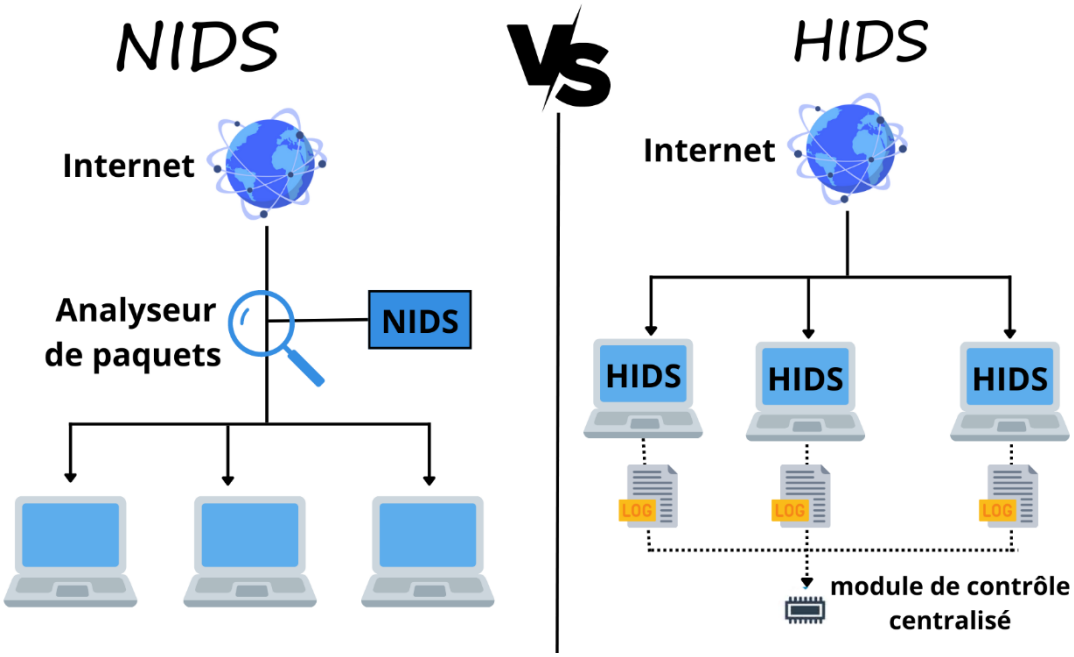

Figure 27: Diagrammes d'architectures NIDS et HIDS.

2.9.2 Signature d'attaque

Nous allons donc examiner spécifiquement comment un IDS fonctionne avec des signatures de paquets. La base de signatures est quasiment la même du côté de l'antivirus et du côté des IDS, cependant pour un IDS open-source, on peut modifier et/ou ajouter des signatures qui seront plus spécifiques à la surveillance. Il est important que la base de

signatures soit mise à jour régulièrement, pour enregistrer les nouvelles signatures d'attaques.

Il est également important de préciser ce qu'est une "anomalie" dans le contexte d'un IDS d'un IDS :

Une anomalie est une activité de paquet inattendue. C'est-à-dire qu'un paquet ayant certaines caractéristiques ne va pas correspondre avec ce que l'on attendait de lui. On peut donc lier les attaques à l'anomalie de paquet. [**Erreur ! Signet non défini.**]

2.9.3 Le but d'avoir un IDS dans un réseau

Le but d'avoir un IDS dans un réseau (généralement LAN) est de surveiller le trafic afin de détecter toute activité suspecte et/ou malveillante contre n'importe quel hôte.. La surveillance du trafic au sein du réseau peut porter autant sur le trafic entrant que celui sortant

2.9.4 Suricata IDS

Suricata est un moteur de détection des menaces réseau open source, il offre des fonctionnalités telles que la détection des intrusions (IDS), la prévention des intrusions (IPS) et la surveillance de la sécurité du réseau. Il fonctionne extrêmement bien avec l'inspection approfondie des paquets et la correspondance des modèles, ce qui le rend incroyablement utile pour la détection des menaces et des attaques. [34]

2.9.5 Format des règles de suricata

En effet, suricata implémente un langage de signature entier, décrit comme étant un ensemble de règles simple, léger flexible et assez puissant pour détecter de nombreuses anomalies dans le trafic qu'il inspecte. Il y a un nombre d'indications simple à se souvenir en développant des règles suricata.

Le premier est que les règles de suricata doivent être complètement contenues sur une seule ligne, l'analyseur de règle de suricata ne sait pas comment traiter des règles sur plusieurs lignes. [34]

Les règles suricata sont divisées en deux sections logiques qui sont :

- L'entête de la règle contient comme informations l'action de la règle, le Protocol, les adresse IP source et destination et les masques réseau, et les ports source et destination.
- Les options de la règle : contient les messages d'alerte et les informations sur la partie du paquet qui doivent être inspectées pour déterminer si l'action de la règle doit être acceptée. [31]

Voici un exemple de règle :

```
alert icmp any any -> any any (msg: "ICMP
packet found"; sid:10004861; rev:1;)
```

Figure 28 Exemple de règle Suricata.

Dans ce qui suit, nous décrirons la signification des propriétés de chaque section comme ce ci :

a L'entête de la règle

L'action : C'est une partie qui nous informe quoi faire quand Suricata trouve un paquet qui correspond aux critères de la règle. En résume quatre actions sont disponibles par défaut dans Suricata.

- **Alerte :** décrit l'action à effectuer. En voici une courte description des options possibles :
  - **Passer :** cela peut être comparé à « accepter » c'est-à-dire que si le paquet correspond à une règle définit, il va être accepté à travers.
  - **Drop :** ici le paquet ne sera pas traité jusqu'à la fin de la chaine. Ignoré, il sera silencieusement supprimé de la pile réseau.
  - **Rejeter :** Il agit de la même manière que drop, le paquet sera retiré de la pile et bloquer.

Le protocole : Utilisé pour la transmission des données, suricata on supporte quatre (si c'est vraiment quatre pourquoi alors etc) : IP, TCP, UDP, ICMP… etc

IP source et destination et ports :

- IP source : **any** : indique l'adresse de l'interface réseau qui écoute le trafic.
- IP destination : **any** : indique l'dresse du réseau externe à écouter.

Les ports : Sont les interfaces d'entrée/sortie sur lesquelles il faudra vérifier les paquets.

- Port source : **any** : indique le port de l'interface réseau qui écoute le trafic.
- Port destination : **any** : indique le port du réseau externe à écouter.

La flèche située entre l'IP et le port indique la direction du flux de paquet qui applique la règle. Presque chaque signature à une flèche vers la droite ce qui signifie que seuls les paquets avec le même sens peuvent égaler.

b Les options de la règle

Msg : affiche un message dans les alertes et journalise les paquets.

Sid : signature ID (identifiant de signature) c'est une valeur unique utilisé pour identifier une règle parmi d'autre et autoriser des notes de version pour chaque règle (REV). [35]

2.10 Conclusion

Ce chapitre nous a permis d'explorer les différents moyens garantissant l'anonymat sur internet particulièrement l'utilisation des réseaux anonymes. Nous avons noté que l'utilisation de ces moyens permettait de contourner les mesures de protection des réseaux locaux et faciliter par conséquent aux utilisateurs l'accès aux parties les plus sombres de l'internet pour y mener potentiellement diverses actions illégales.

En outre, nous avons étudié également les techniques d'inspection de paquets appelée "Deep Packet Inspection" ainsi que les systèmes de détection d'intrusion et ce, afin de nous aider à mettre en œuvre la solution idoine, qui sera décrite dans le prochain chapitre, pour lutter contre ce genre d'intrusion.

Chapitre 3 Détection de l'usage du réseau Jondonym

3.1 Introduction

JonDonym est un réseau anonyme qui permet aux utilisateurs d'accéder au DarkWeb et de mener potentiellement des activités malveillantes contre des individus et des organisations. Par conséquent, la détection de l'utilisation du réseau JonDonym dans une entreprise est nécessaire pour lutter contre l'utilisation de ce type de réseau.

A ce titre, nous proposons dans le cadre de notre travail une solution qui consiste à Repérer l'utilisation du JonDoBrowser et de l'application ANONdroid à travers les différentes étapes ci-après et qui seront détaillés dans ce chapitre :

1. La capture des paquets venant du navigateur JonDoBrowser avec un outil d'analyse approfondie des paquets" Deep Packet Inspection ".
2. l'analyse détaillée des paquets capturés.
3. L'extraction des empreintes numérique du réseau anonyme JONDONYM.

3.2 L'objectif de notre recherche

Notre recherche a pour but de contrer l'utilisation de JonDonym dans un réseau d'entreprise, en implémentant des règles IDS sous « Suricata » à partir des empreintes numériques qu'on a extraites à partir de l'analyseur de paquets « Wireshark ».

3.3 Plan de travail

Pour parvenir à notre but nous avons adopté les démarches suivantes :

- **L'étude théorique :** Cette phase a été consacrée à l'étude du réseau anonyme JonDonym notamment son principe de fonctionnement.

- **Capture :** La détection de l'utilisation d'un réseau anonyme passe par l'extraction des empreintes numériques de ce dernier en analysant le trafic réseau. Pour cela, nous avons utilisé l'analyseur de paquets "Wireshark" pour extraire plusieurs informations des paquets capturés lors de l'utilisation de JonDonym.
- **L'analyse :** Après avoir capturé le trafic réseau lors de l'utilisation de JonDonym, nous avons procédé à l'analyse de ces paquets en les comparants avec des paquets capturés sans l'utilisation du dit réseau anonyme. Cette comparaison nous a permis d'extraire les empreintes JonDonym.
- **Détection :** Enfin, dans la dernière étape, nous avons utilisé les empreintes numériques pour créer des règles IDS " Suricata " qui permettent de détecter l'utilisation du navigateur JonDoBrowser et de l'application ANONdroid (la version APK de JAP) dans le réseau LAN.

3.4 Matériels utilisés

Les moyens suivants ont été utilisés pour mener à bien notre recherche :

Tableau 7: **Equipements et logiciels utilisés " PC serveur "**

	Matériaux	**Logiciels**
PC serveur	Un ordinateur portable HP avec un processeur Intel (R) Core (TM) i3-7020U@ 2.30 GHz x 4 avec une RAM de 8.00 GiB, fonctionnant sous le système d'exploitation Linux Ubuntu 20.04 LTS 64 bits.	- Wireshark version 3.2.3 (64-bits). - Suricata version : 6.0.4

Tableau 8: Equipements et les logiciels utilisés " client "

	Matériaux	**Logiciels**
Client 1	Un ordinateur portable HP avec un processeur Intel (R) Core (TM) i3-7020U@ 2.30 GHz x 2 avec une RAM de 4.00 GiB, fonctionnant sous le système d'exploitation Windows 10 Professional version 21H2 64 bits.	- JonDoBrowser (JonDoFox) version : 7.5.9.14 - Jondo (JAP) version : 00.20.010-beta - Navigateur Mozilla Firefox version 101 - Navigateur Google Chrome version 102.0.5005.115 (build officiel) (64-bit)
Client 2	Smartphone Redmi Note 8 Pro avec un CPU Octa-Core MAX2.05 GHZ avec une RAM de 6.00 Go, fonctionnant sous Android 11 RP1A.200720.011	- l'application ANONdroid version : 00.00.030

3.5 Environnement

3.5.1 Architecture client/ serveur

Lors de notre recherche, nous avons réalisé une architecture client/serveur, dans laquelle :

a Le PC serveur

Était équipé de deux interfaces réseaux :

La première interface, configurée avec l'adresse : 192.168.8.101, a été connectée à l'Internet via un routeur doté d'un câble Ethernet.

La deuxième interface, configurée avec l'adresse : 10.42.0.1, a été connectée au réseau local via le point d'accès.

Pour l'ordinateur administrateur (serveur) on a utilisé le système d'exploitation Ubuntu 20.04 Linux. Ubuntu est un système d'exploitation Linux facile à utiliser qui a trouvé sa place dans le monde entier. Le meilleur de tous, Ubuntu est tout à fait gratuit, y compris les mises à jour futures. Il est également extrêmement léger sur le PC.

b Les clients

Les pc clients se connectent à Internet via le point d'accès WIFI et en passant par la passerelle (le PC serveur).

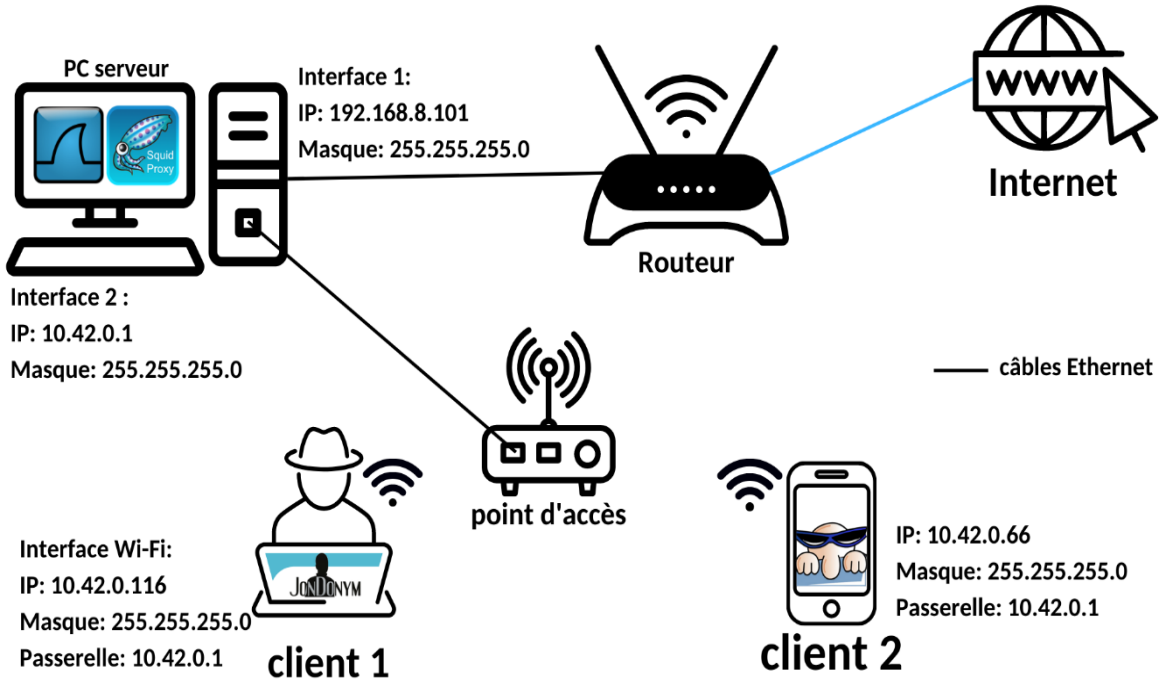

Figure 29: Architecture client/serveur.

- **Client 1 :** Pour la navigation en réseau jondonyme, deux composants sont nécessaires :

- **JonDo (anciennement JAP) :** est l'outil proxy de changement d'IP utilisé pour connecter l'utilisateur au réseau JonDonym. Il agit comme un proxy et transmettra le trafic des applications internet cryptées multiple aux cascades de Mix et ainsi, il

cachera l'adresse IP. Il s'agit d'une application Java, open source disponible gratuitement. Vous pouvez utiliser JonDonym gratuitement, mais les cascades de mixage gratuites sont limitées dans certains cas. La vitesse complète et les fonctions d'anonymisation ne sont disponibles qu'avec un compte premium.

Figure 30 Logo du logiciel Jondo.

- **JonDoBrowser (JonDoFox) :** est un navigateur web qui inclut déjà le client JonDo et toutes les fonctions d'anonymisation nécessaires. Il est particulièrement conçu pour une navigation anonyme et sécurisée et est basé sur le navigateur Tor.

Figure 31 Logo du navigateur JondoBrowser.

Remarque : Les deux applications sont disponibles sur le site https://anonymous-proxy-servers.net/index.html , ainsi que la documentation y afférentes.

- **Client 2 :** Les utilisateurs du système Android devront installer l'application ANONdroid, disponible sur Play Store, pour naviguer sur le réseau Jondonyme.

Figure 32 Logo de l'APK ANONdroid.

3.6 Installation d'un serveur proxy

Sur le PC administrateur, fonctionnant sous le système d'exploitation Ubuntu 20.04, nous avons installé un serveur proxy pour établir une politique de contrôle qui consiste à définir les sites auxquels les utilisateurs n'ont pas le droit de consulter. Pour cela, nous avons choisi Squid proxy.

3.6.1 Installer Squid sur Ubuntu Linux

Pour commencer, nous avons téléchargé Squid proxy, en exécutant la ligne de commande suivante :

$ sudo apt -y install squid

La commande suivante permet d'installer le serveur Squid proxy :

$ sudo yum install squid

Ensuite, pour lancer le proxy, commande suivante est exécutée :

$ systemctl start squid

Pour configurer les règles sur Squid Proxy, nous ouvrons le fichier squid.conf dans un éditeur de texte à travers la commande suivante :

$ sudo nano /etc/squid/squid.conf

Puis nous avons bloqué l'accès au réseau social Facebook dans notre LAN.

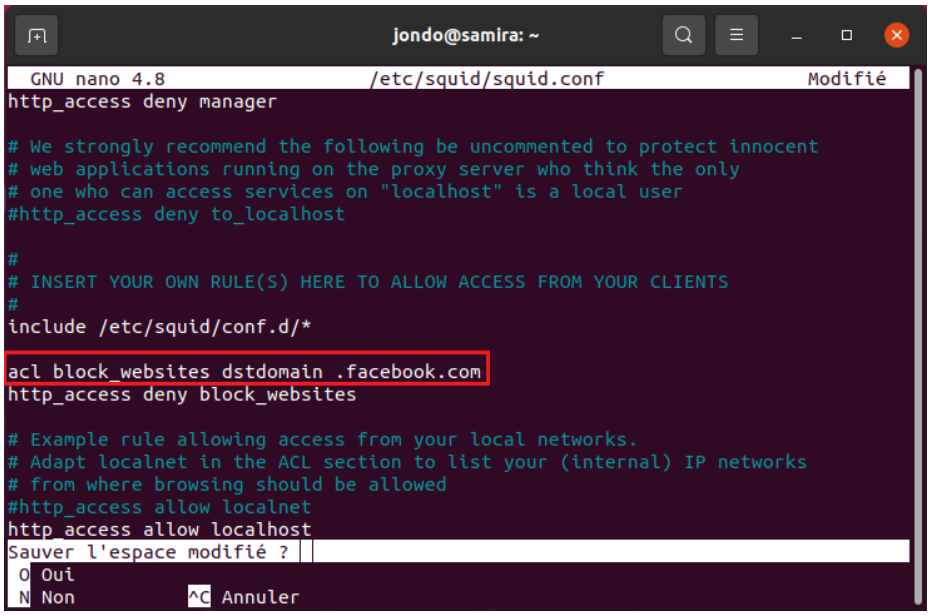

Figure 33: Bloque de Facebook sur squid proxy.

3.6.2 Accéder à facebook.com

Après avoir installé le Squid proxy, et l'avoir configuré de manière à bloquer l'accès au site Facebook, nous avons essayé de vérifier que le verrou fonctionnait bien en procédant comme suit sur le PC client :

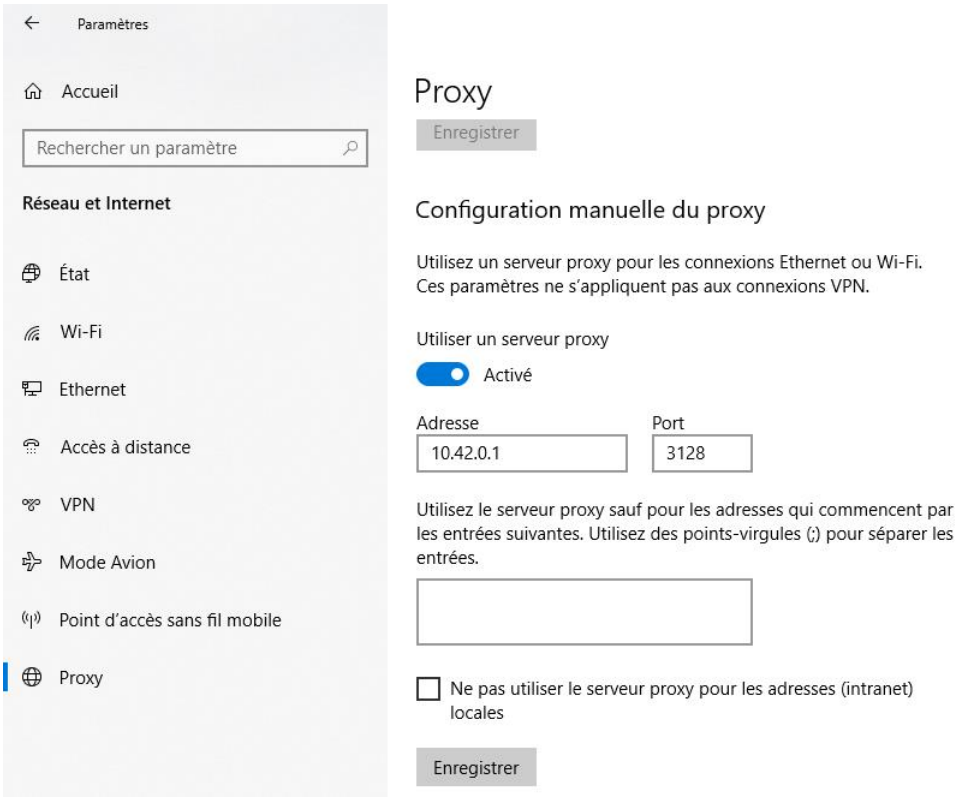

Figure 34: Activé le proxy sur le PC client.

L'adresse 10.42.0.1 est l'adresse (passerelle) du PC serveur comme déjà mentionné.

Le port 3128 est le port utilisé par le Squid proxy.

Nous avons ensuite tenté d'accéder à facebook.com par le navigateur Google Chrome ou nous avons constaté que celui-ci était bloqué.

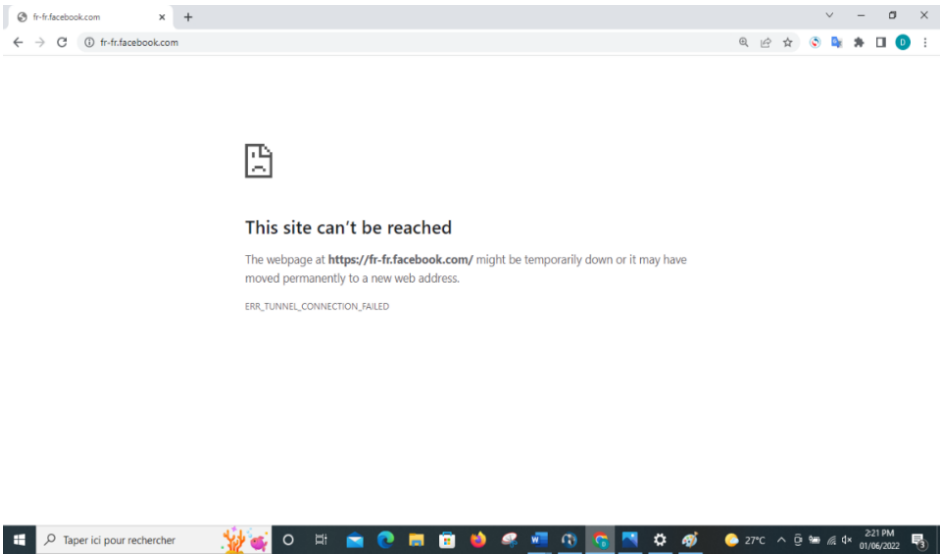

Figure 35: Accès à facebook.com via le navigateur Google Chrome.

La même expérience a été refaite mais cette fois-ci en utilisant le réseau JonDonym. Pour ce faire, nous nous sommes connectées d'abord au logiciel Jondo qui se charge de nous connecter au réseau de Mix JonDonym.

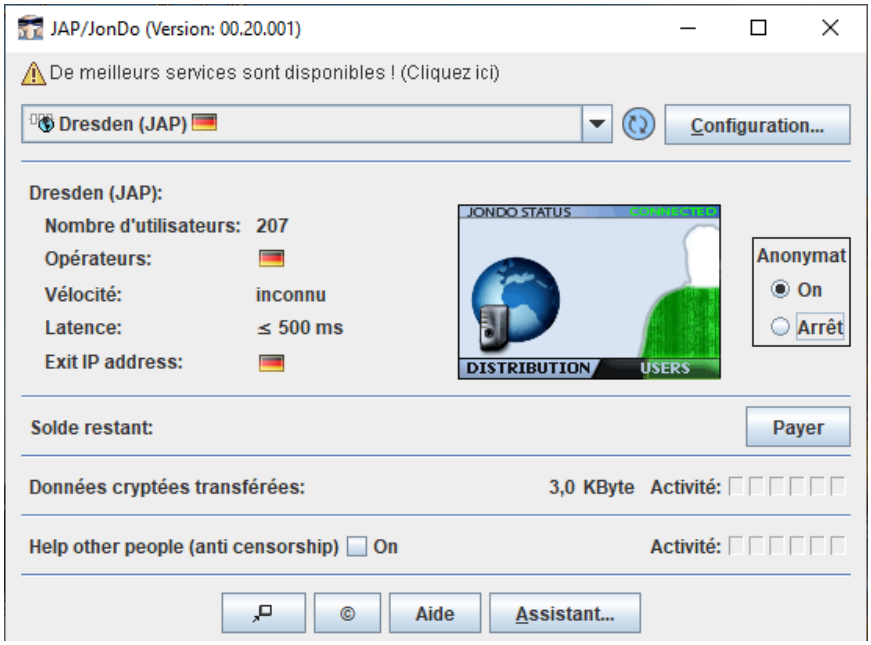

Figure 36: connexion au logiciel Jondo.

Ensuite, en utilisant le JondoBrowser nous nous connectons à facebook.com

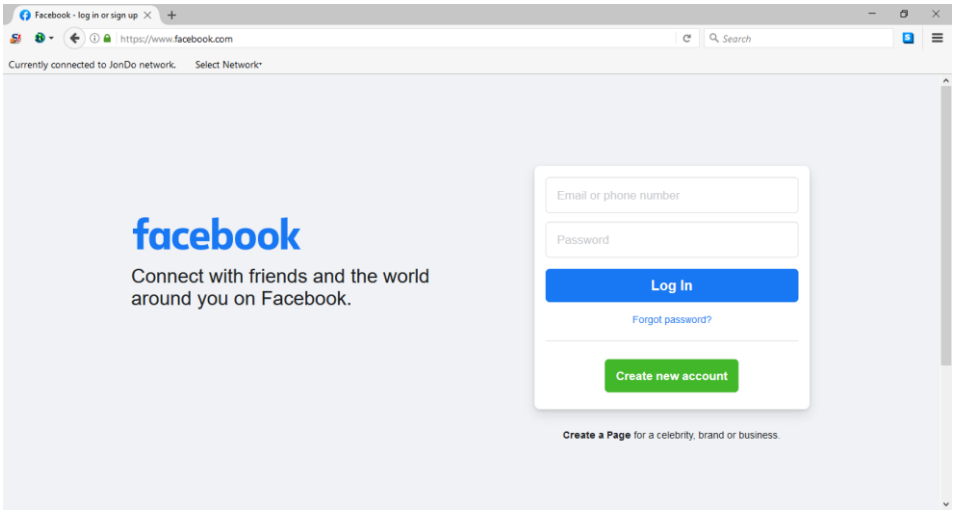

Figure 37: Accès à facebook.com via le navigateur JondoBrowser.

JonDonym a réussi à se connecter à www.facebook.com bien que celui-ci soit bloqué ! Ceci constitue une violation aux règles de sécurité que nous avons créées et peut compromettre par conséquent toute la sécurité de notre système

Nous commençons donc notre recherche pour détecter l'utilisation du réseau JonDonym.

3.7 Analyse et capture du trafic réseau

Pour commencer, nous avons capturé et étudié les paquets TCP (SYN, SYN ACK, ACK) ainsi que les paquets TLS (SSL) afin de pouvoir les comparer dans le but d'extraire les empreintes digitales du réseau JONDONYM. Pour cela, nous avons choisi l'analyseur de paquets Wireshark afin de capturer le trafic réseau sur le site suivant :

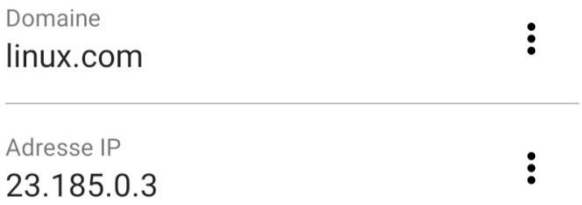

Figure 38: IP du site linux.com

Le trafic a été capturé lors de la connexion à linux.com avec trois navigateurs (Google Chrome, Firefox, Jondonym).

3.7.1 Capture du trafic réseau

En se connectant au site www.linux.com avec le navigateur google chrome les paquets suivants ont été capturés :

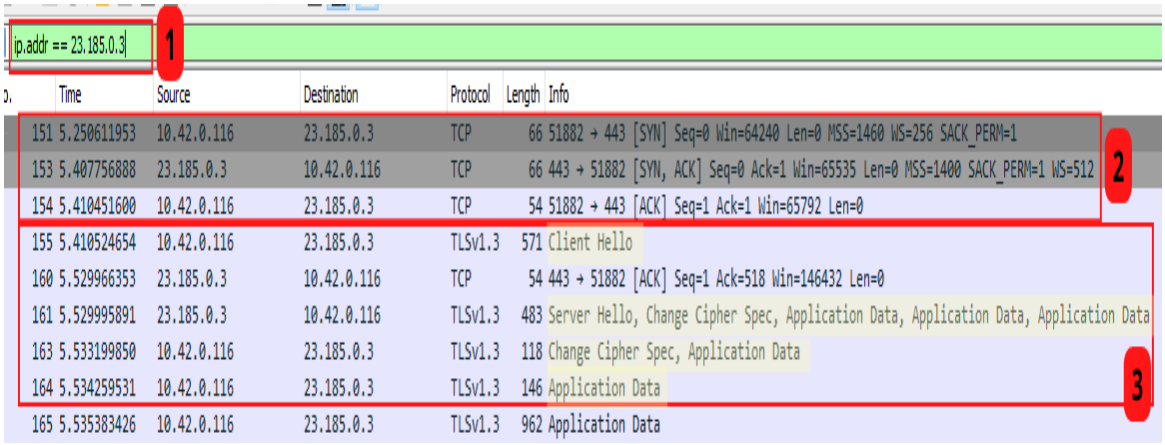

Figure 39: capture Wireshark navigateur Google Chrome.

- Section 1 sur la figure : nous avons appliqué le filtre d'affichage "ip.addr == 23.185.0.3" pour montrer uniquement les paquets provenant de cette adresse (l'adresse ip du site linux .com).
- Section 2 de la figure : affiche la liste des paquets capturés durant la connexion TCP "Three Way Handshake".
- Section 3 sur la figure : affiche le paquet TLS capturé lors de la connexion.

Nous effectuons la même opération avec le navigateur Firefox, et on a eu le même comportement.

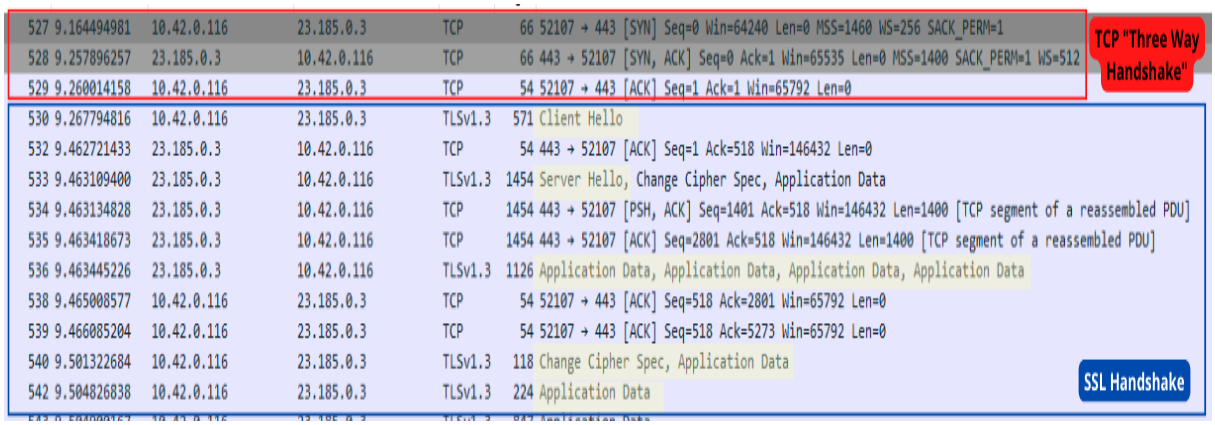

Figure 40: Capture Wireshark navigateur Firefox.

Pour faire la même opération avec Jondonym, il faut d'abord se connecter au logiciel JONDO, voici les captures que nous avons eu :

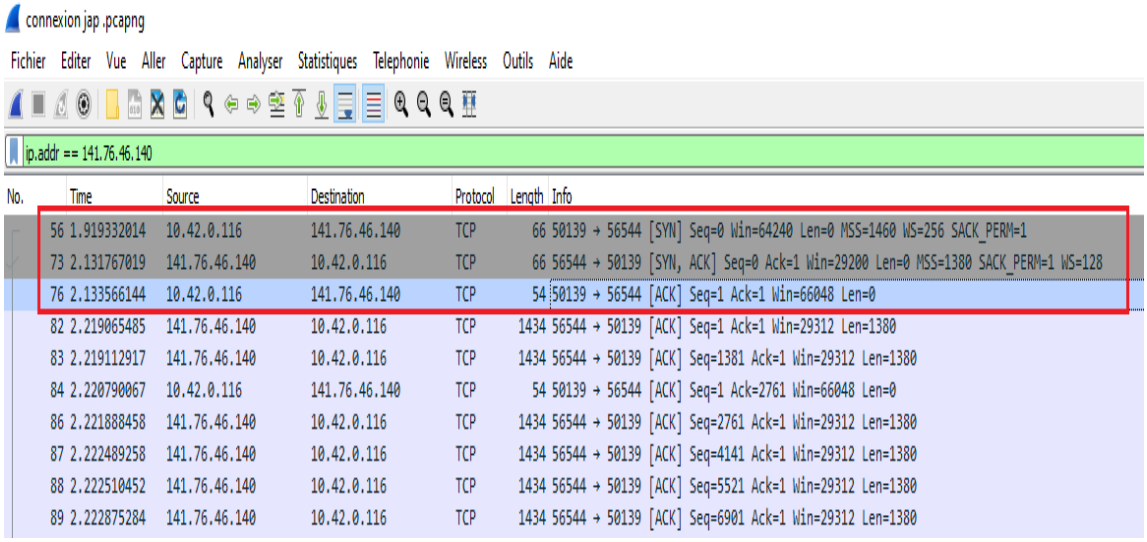

Figure 41: capture Wireshark connexion au logiciel Jondo.

Nous constatons que le logiciel Jondo contacte une adresse IP spécifique 141.76.46.140.

Ensuite, nous accédons au site linux.xom en utilisant le JondoBrowser. Voici les captures obtenues à partir de Wireshark :

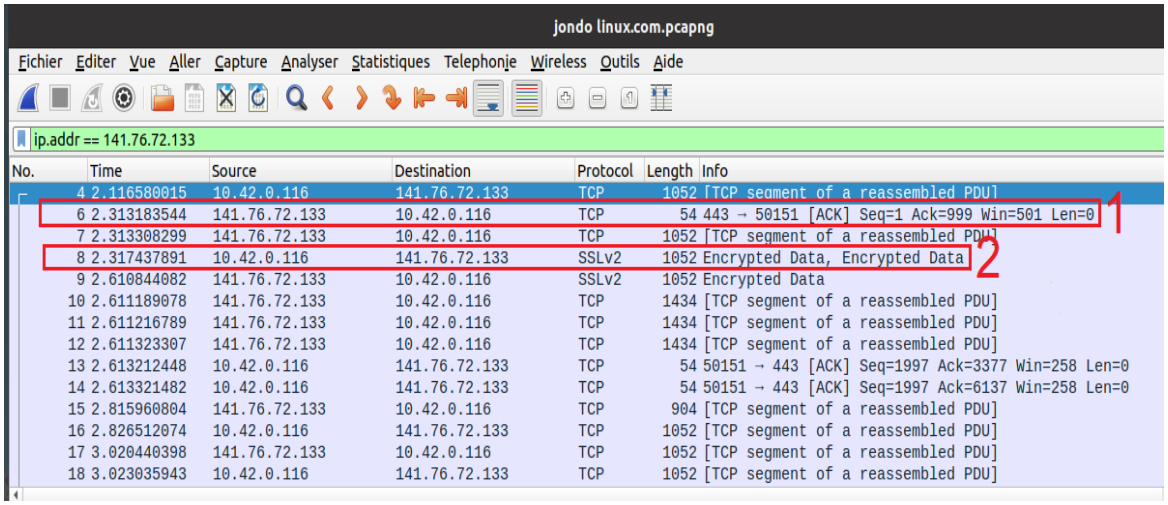

Figure 42: capture Wireshark navigateur Jondobrowser.

- Section 1 sur la figure : affiche le paquet capturé durant la connexion TCP "ACK".
- Section 2 de la figure : affiche le paquet capturé durant la connexion SSL.

Le logiciel Jondo contacte une adresse IP spécifique 141.76.72.133 au lieu de l'adresse 23.185.0.3 correspondante au site linux.com.

Contrairement aux autres navigateurs, nous déduisant que lorsque nous utilisons Jondobrowser, les paquets "SYN et SYN-ACK" sont cachés et nous ne pouvons pas les voir dans wireshark, nous ne voyons que le paquet ACK. De plus, les paquets "SSL Handshake" sont masqués aussi et nous ne voyons que le paquet Encrepted Data.

Après les recherches de l'adresse IP 141.76.72.133, nous avons trouvé que c'est l'adresse du serveur mix du réseau JonDonym.

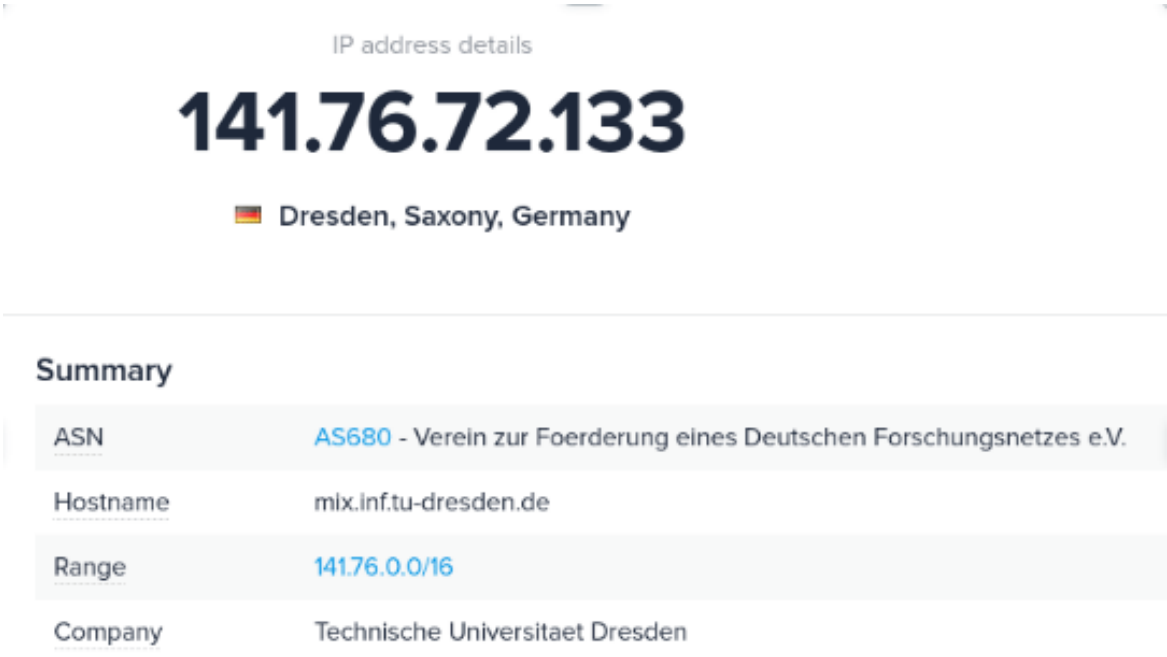

Figure 43: l'adresse du serveur Mix du réseau jondonym.

3.7.2 Analyse des paquets capturés

Dans cette phase, nous allons analysé les paquets capturés lors des connexions établies entre les navigateurs et le site linux.com, après avoir analysé les paquets, nous allons faire une comparaison entre les trois navigateurs (Google Chrome, Firefox, Jondobrowser).

Cette étape nous a permis à extraire les informations suivantes :

- **Longueur totale :** la taille du paquet ou de la trame pour être plus précis.
- **Identification :** numéro permettant d'identifier les fragments d'un même paquet.

- **TTL :** Le champ TTL (Time To Live) indique la durée de vie maximale du paquet.
- **Port source :** correspond au port relatif à l'application en cours sur la machine source.
- **Port destination :** correspond au port relatif à l'application en cours sur la machine de destination.
- **Numéro de séquence :** correspond au numéro du paquet. Cette valeur permet de situer à quel endroit du flux de données le paquet, qui est arrivé, doit se situer par rapport aux autres paquets.
- **Stream index :** affiche un numéro unique pour chaque flux, tel que 1 pour le premier flux, 2 pour le deuxième flux, etc. Un flux est une collection connexe de paquets TCP, commençant généralement par la poignée de main à trois, puis le transfert de données, et se terminant par la fermeture de la session.
- **Flags :** indique l'état de la fragmentation.
- **Windows size value :** window size value est la partie la plus importante de l'en-tête TCP. Ce champ est utilisé par le récepteur pour indiquer à l'expéditeur la quantité de données qu'il peut accepter. Ce champ est donc très important pour le transfert efficace des données et le contrôle du flux.

  La taille de la fenêtre utilise l'octet comme unité de mesure. Si la taille de la fenêtre est de 60k, cela signifie que le récepteur accepte 60 kilobytes de données. Lorsque les données transmises atteignent la valeur de la fenêtre, l'expéditeur attend une autre valeur de fenêtre de la part du récepteur, ainsi que l'accusé de réception de la fenêtre qui vient d'être reçue. [36]
- **Checksum :** représente la validité du paquet de la couche 3.

Nous débutons la comparaison avec le paquet ACK de la connexion TCP

Tableau 9: Comparaison entre les trois navigateurs du paquet ACK.

	Google Chrome	Firefox	Jondobrowser
Type	IPv4 (0x0800)	IPv4 (0x0800)	IPv4 (0x0800)
Total Length	40	40	40
Identification	0x34c2 (13506)	0x3708 (14088)	0xb07c (45180)
TTL	128	128	43
Protocole	TCP (6)	TCP (6)	TCP (6)
Port source	51882	52107	443
Port destination	443	443	50151
Numéro de séquence	1	1	1
Stream index	3	29	1
Flags	0x010 (ACK)	0x010 (ACK)	0x010 (ACK)
Windows size value	257	257	501
Checksum	0x7c89	0xf967	0x7d63

a Observations

- **Identification :** Nous remarquons que la valeur change d'un navigateur à l'autre. Cette différence est absolument normale, car chaque connexion doit être identifiée de manière unique.
- **Port source/destination :** d'une application à l'autre, le port change de façon aléatoire.
- **Stream index :** La valeur varie pour chaque paquet, mais nous ne pouvons pas tenir compte de ce changement car il s'agit d'un mappage interne de Wireshark.
- **Checksum :** Nous observons que sa valeur change d'un navigateur à l'autre, c'est donc un critère incomparable pour extraire les empreintes digitales.

- **TTL :** fait référence à la durée pendant laquelle un paquet est censé exister dans un réseau avant d'être écarté par un routeur. Il varie d'un paquet à l'autre et ne peut donc pas être considérée comme une signature.
- **Windows size value :** est une indication de la quantité de données (en octets) que le dispositif récepteur est prêt à recevoir à un moment donné. Le dispositif récepteur peut utiliser cette valeur pour contrôler le flux de données, ou comme mécanisme de contrôle de flux. Nous remarquons qu'il ne change que pour le JondoBrowser, c'est donc une signature intéressante.

Ensuite, nous passons à la comparaison du paquet Application Data du SSL Handshake.

Tableau 10: Comparaison entre les trois navigateurs du paquet SSL Handshake.

	Google Chrome	Firefox	Jondobrowser
Type	IPv4 (0x0800)	IPv4 (0x0800)	IPv4 (0x0800)
Total Length	557	557	1038
Identification	0x34c3 (13507)	0x3709 (14089)	0x315d (12637)
TTL	128	128	128
Protocole	TCP (6)	TCP (6)	TCP (6)
Port source	51882	52107	50151
Port destination	443	443	443
Numéro de séquence	1	1	999
Stream index	3	29	1
Flags	0x018 (PSH, ACK)	0x018 (PSH, ACK)	0x018 (PSH, ACK)
Windows size value	257	257	258
Checksum	0xbcbd	0xa3e7	0x0cee

Les seules valeurs qui ne changent qu'en utilisant jondobrowser sont : Total Length, Numéro de séquence, Windows size value. Dans ce cas, nous allons les utiliser pour extraire des empreintes numériques et les implémenter dans le système de détection d'intrusion Suricata pour détecter toute connexion au réseau.

3.8 Extraction des empreintes numériques

En comparant les différentes communications, nous devons extraire les éléments spécifiques à Jondonym afin de les détecter. Nous allons extraire de ces éléments une empreinte numérique qui identifie l'utilisation de Jondonym.

a Total Length

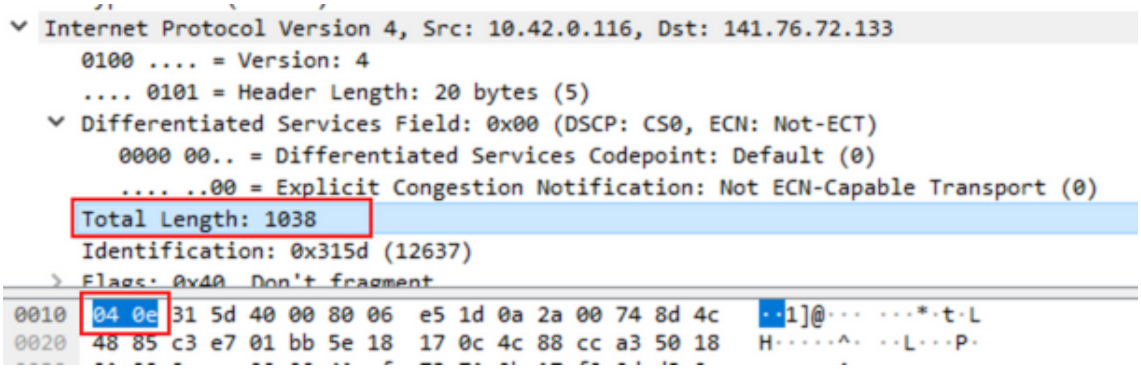

Figure 44: L'empreinte Total Length.

La signature Total Length est le code suivant (code en hexadécimal) :

04 0e

b Numéro de séquence

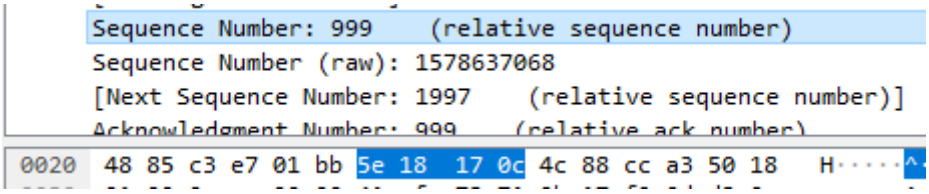

Figure 45: L'empreinte Numéro de séquence.

La signature Numéro de séquence est le code suivant (code en hexadécimal) :

5e 18 17 0c

c *Windows size value*

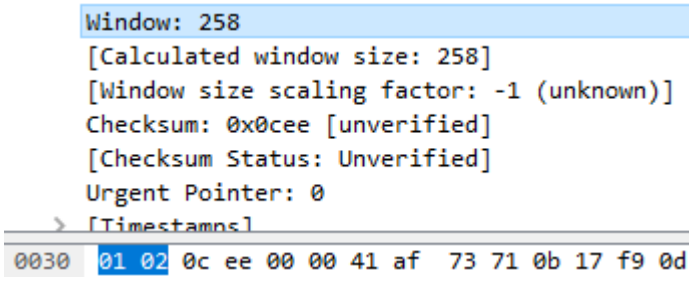

Figure 46: L'empreinte Windows size value.

La signature Windows size value est le code suivant (code en hexadécimal) :

```
01 02
```

3.9 Détection de Jondonym

3.9.1 Création des règles Suricata

Nous avons utilisé les empreintes digitales pour créer des règles suricata afin de pouvoir repérer un trafic réseau malveillant (réseau Jondonym).

La première règle identifie le Total Length, cette règle lancera une alerte en indiquant le message " ATTENTION TENTATION DE CONNEXION JONDONYM Total Length ".

```
alert tcp any any -> [141.76.72.133,141.76.46.140] any (msg: "ATTENTION TENTATION DE CONNEXION JONDONYM Total length"; content: "|04 0e|" ; sid:1;)
```

La deuxième règle identifie le Numéro de séquence, cette règle lancera une alerte en indiquant le message " ATTENTION TENTATION DE CONNEXION JONDONYM Sequence number ".

```
alert tcp any any -> [141.76.72.133,141.76.46.140] any (msg: "ATTENTION TENTATION DE CONNEXION JONDONYM Sequence number"; content: "|5e 18 17 0c|"; sid:2;)
```

La troisième règle identifie Windows size value, cette règle lancera une alerte en indiquant le message " ATTENTION TENTATION DE CONNEXION JONDONYM Windows size value".

```
alert tcp any any -> [141.76.72.133,141.76.46.140] any (msg: "ATTENTION TENTATION DE CONNEXION JONDONYM Window size value"; content: "|01 02|"; sid:3;)
```

Dans la partie qui indique l'adresse du réseau externe à écouter de la règle Suricata, nous avons spécifié les deux adresses [141.76.72.133,141.76.46.140] afin de ne pas avoir de fausses alertes, car ces deux adresses sont celles que nous avons notées dans la partie capture que Jondobrowser et le logiciel Jondo contactent toujours.

3.9.2 Installation de Suricata

Nous avons utilisé les lignes de commande suivantes pour installer Suricata :

$ sudo apt install suricata

Ensuite, nous avons accepté la garantie de l'installation.

Le fichier de configuration se trouve dans /etc/suricata/suricata.yaml, et les règles se trouvent dans /etc/suricata/rules/

3.9.3 Implémentation des règles dans Suricata

Nous avons implémenté les règles dans le fichier my2.rules que nous avions créé à l'aide de la commande :

$ toch /etc/suricata/rules/my2.rules

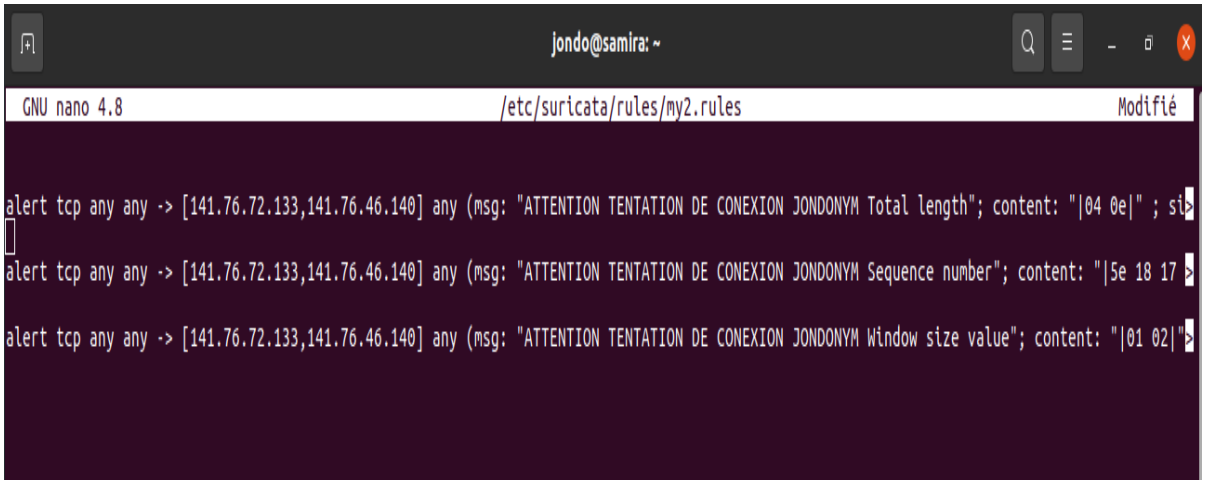

Figure 47: Implémentation des règles dans le fichier my2.rules.

3.9.4 Détection du réseau anonyme JONDONYM

- Lancer Suricata en utilisant la commande suivante :

  $ sudo service suricata start

- Vérifier le statut de Suricata, s'il est actif ou non, pour nous assurer que Suricata est en marche. On exécute la commande suivante :

  $ systemctl status suricata

```
jondo@samira:~$ systemctl status suricata
● suricata.service - LSB: Next Generation IDS/IPS
     Loaded: loaded (/etc/init.d/suricata; generated)
     Active: active (running) since Sat 2022-06-18 15:53:56 CET; 33s ago
       Docs: man:systemd-sysv-generator(8)
    Process: 8666 ExecStart=/etc/init.d/suricata start (code=exited, status=0/SUCCESS)
      Tasks: 10 (limit: 9356)
     Memory: 56.7M
     CGroup: /system.slice/suricata.service
             └─8675 /usr/bin/suricata -c /etc/suricata/suricata.yaml --pidfile /var/run/suricata.pid --af-packet -D -vvv

15:53:56 18 جوان samira systemd[1]: Stopped LSB: Next Generation IDS/IPS.
15:53:56 18 جوان samira systemd[1]: Starting LSB: Next Generation IDS/IPS...
15:53:56 18 جوان samira suricata[8666]: Likely stale PID 8441 with /var/run/suricata.pid exists, but process is not running!
15:53:56 18 جوان samira suricata[8666]: Removing stale PID file /var/run/suricata.pid
15:53:56 18 جوان samira suricata[8666]: Starting suricata in IDS (af-packet) mode... done.
15:53:56 18 جوان samira systemd[1]: Started LSB: Next Generation IDS/IPS.
jondo@samira:~$
```

Figure 48: Status suricata active.

a Architecture de détection finale

A la fin de notre étude, voici l'architecture client/serveur que nous avons réalisée :

Dans le PC serveur nous avons installé Suricata IDS, squid proxy. Tout le trafic en provenance du PC client passe par le PC serveur pour être détecté par l'IDS Suricata.

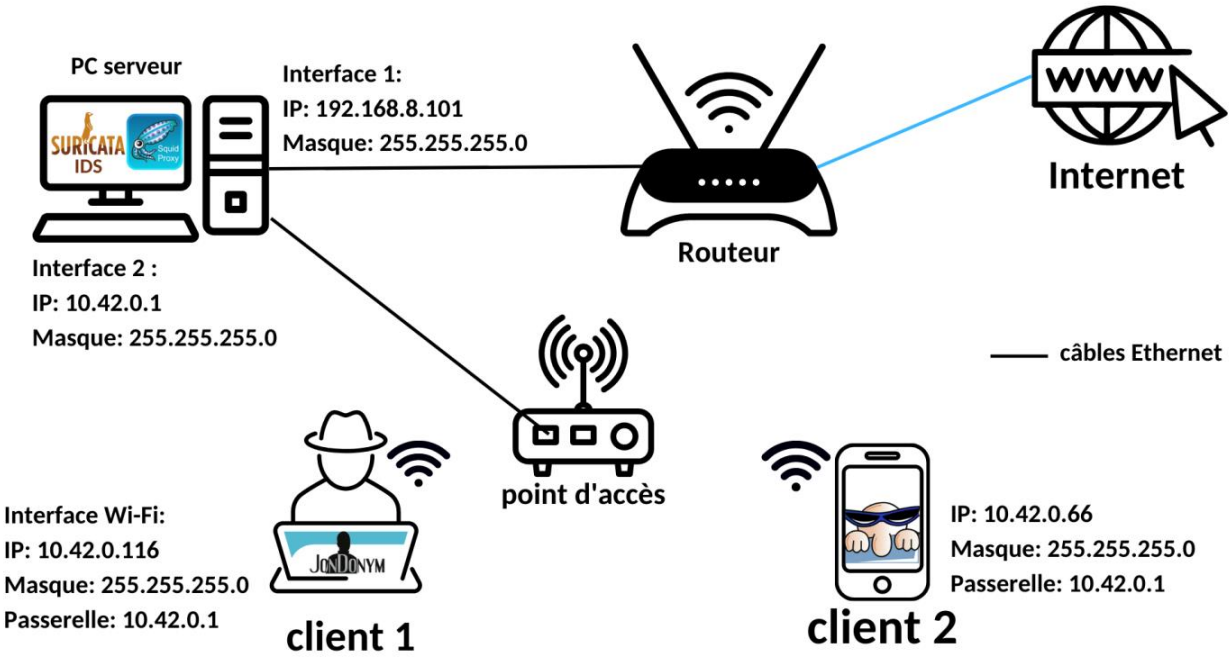

Figure 49: Architecture de détection finale.

b Lancement de la détection

Pour consulter le fichier d'alertes de Suricata, il faut exécuter la commande suivante

$ tail -f /var/log/suricata/fast.log

```
05/29/2022-11:48:27.135012  [**] [1:3:0] ATTENTION TENTATION DE CONEXION JONDONYM Window size value [**] [Classification: (null)] [Priority: 3
] {TCP} 193.55.61.150:80 -> 10.42.0.222:52487
05/29/2022-12:32:01.566995  [**] [1:1:0] ATTENTION TENTATION DE CONEXION JONDONYM Total length [**] [Classification: (null)] [Priority: 3] {TC
P} 10.42.0.11:61815 -> 141.76.72.133:443
05/29/2022-12:32:35.810926  [**] [1:3:0] ATTENTION TENTATION DE CONEXION JONDONYM Window size value [**] [Classification: (null)] [Priority: 3
] {TCP} 10.42.0.116:52064 -> 141.76.72.133:443
05/29/2022-12:32:38.931148  [**] [1:1:0] ATTENTION TENTATION DE CONEXION JONDONYM Total length [**] [Classification: (null)] [Priority: 3] {TC
P} 10.42.0.116:52064 -> 141.76.72.133:443
```

Figure 50: Le fichier d'alertes de Suricata.

Nous pouvons constater que le Suricata inspecte déjà notre interface réseau et génère par conséquent des alertes. De plus, les alertes affichent la date à laquelle elles se sont produites et une brève description de l'alerte.

Pour mieux afficher les alertes, et faciliter la lecture nous avons installé une interface graphique et reliée cette dernière à Suricata.

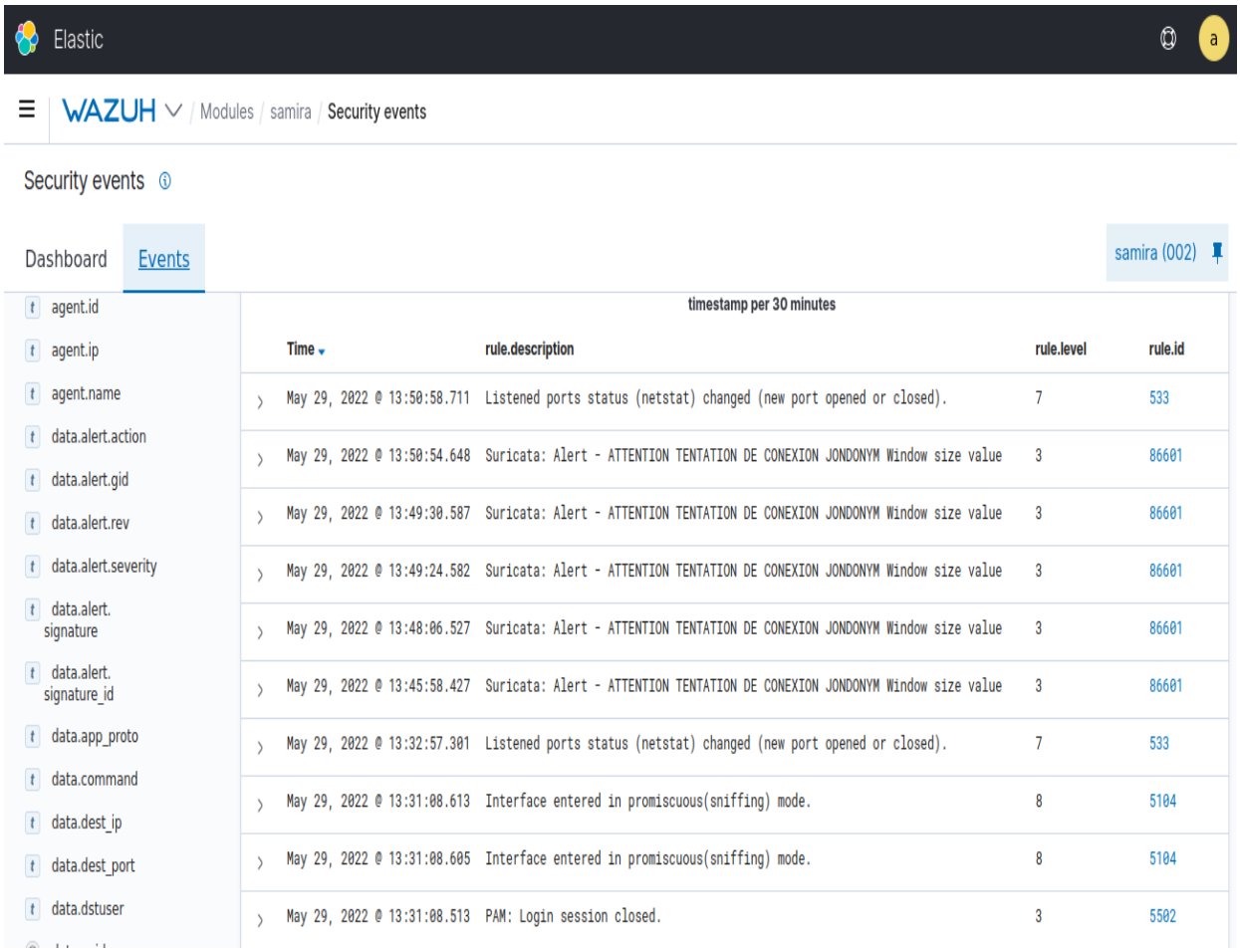

Figure 51: Interface graphique.

t data.src_ip	10.42.0.66
t data.src_port	57236
data.timestamp	Jun 18, 2022 @ 16:20:56.693
t decoder.name	json
t id	1655565657.14848
t input.type	log
t location	/var/log/suricata/eve.json
t manager.name	wazuh-manager
t rule.description	Suricata: Alert - ATTENTION TENTATION DE CONEXION JONDONYM Window size value
# rule.firedtimes	1
t rule.groups	ids, suricata

Figure 52: Les détails d'une alerte.

Comme nous montre l'image ci-dessus, Suricata a lancé une alerte indiquant le message "ATTENTION TENTATION DE LA CONNEXION JONDONYM Valeur de la taille de Windows" pour l'adresse IP 10.42.0.66 (l'adresse IP de notre client Android) de là nous constatons que nos règles sont également valables pour l'application ANONdroid (version APK de Jondo).

	Time	rule.description	rule.level	rule.id
›	Jun 19, 2022 @ 17:42:32.755	Suricata: Alert - ATTENTION TENTATION DE CONEXION JONDONYM Total length	3	86601
›	Jun 18, 2022 @ 16:20:57.004	Suricata: Alert - ATTENTION TENTATION DE CONEXION JONDONYM Window size value	3	86601
›	Jun 18, 2022 @ 15:59:57.899	Suricata: Alert - ATTENTION TENTATION DE CONEXION JONDONYM Total length	3	86601
›	Jun 11, 2022 @ 11:21:58.142	Successful sudo to ROOT executed.	3	5402
›	Jun 11, 2022 @ 11:01:51.276	Suricata: Alert - ATTENTION TENTATION DE CONEXION JONDONYM Window size value	3	86601
›	Jun 11, 2022 @ 10:24:01.575	Successful sudo to ROOT executed.	3	5402

Figure 53: Les alertes lancées par Suricata.

Cette figure nous montre toutes les alertes générées pendant la période du 11 juin au 19 juin, ce qui nous permet de déduire que nous n'avons pas de fausses alertes. De plus, nous remarquons que Suricate ne génère que deux alertes (Window size value, Total Length) l'alerte du sequence number n'apparaît jamais.

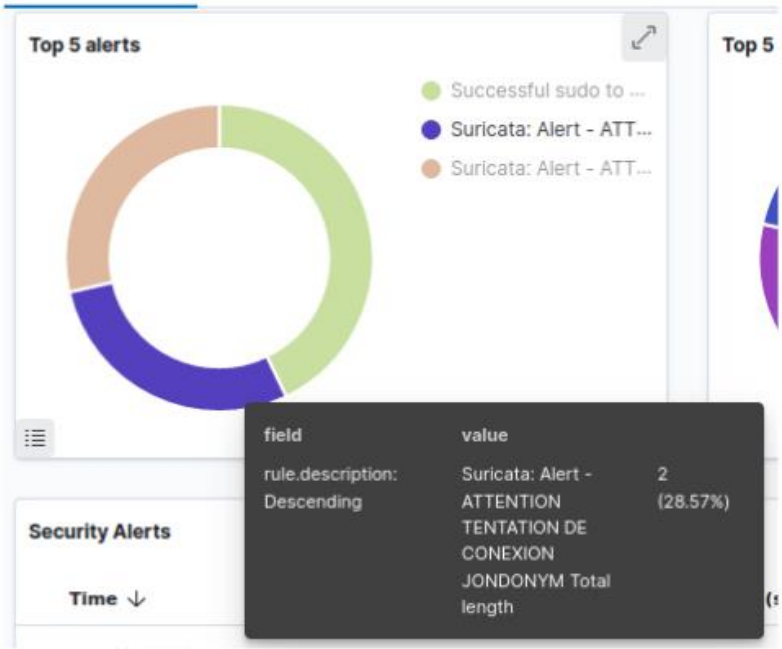

Figure 54: Alerte la plus générée.

Le diagramme de la figure 52, nous montre le taux d'alerte le plus élevé (Total length).

3.10 Discussion

- Le JondoBrowser et l'APK ANONdroid ont été détectés en utilisant les mêmes règles car ils passent par le même réseau (le réseau JonDonym).
- Les deux règles Window size value, Total Length implémentées dans Suricata impliquent des alertes, ces règles sont fiables et ne génèrent pas de fausses alertes.
- La règle du Numéro de séquence n'implique pas d'alertes, elle n'est donc pas fiable.
- Le taux de détection est 100% sans fausses alertes.
- L'alerte Total Length est la plus générée, avec un taux de 28.57%
- La génération des alertes n'est pas en temps réel ; nous avons noté un petit retard lors de la détection du réseau jondym car il passe par les réseaux MixNetWorks (réseau de Mix) qui est la famille de modes de routage supportant l'anonymat par l'utilisation de multiples serveurs intermédiaires re-routant l'information.

3.11 Conclusion

Dans ce chapitre, nous avons analysé le trafic provenant du JondoBrowser. Cette analyse nous a permis d'extraire des empreintes numériques suite à une comparaison entre les paquets "TCP Handshake" et "TLS Handshake". Nous avons pu extraire trois empreintes digitales qui peuvent être mises en œuvre sous un système de détection d'intrusion IDS.

Nous avons alors créé des règles à partir des empreintes extraites, puis les avons implémentées dans l'IDS Suricata afin de détecter l'utilisation du réseau Jondonym dans un réseau d'entreprise.

Les résultats des tests effectués avec ces règles ont confirmé la fiabilité de celles-ci. Nous pouvons donc affirmer que notre étude permet de détecter avec succès les connexions au réseau Jondonym.

Conclusion générale

La vie privée constitue l'un des droits fondamentaux. Elle se trouve aujourd'hui plus que jamais menacée par une surveillance électronique massive exercée par des institutions et des organismes afin de nuire ou d'influencer les populations.

Des outils ont vu le jour pour garantir le respect de la vie privée et l'anonymat sur internet. Toutefois ils utilisent des techniques permettant de contourner les mesures de sécurité imposées par les réseaux en particulier les réseaux d'entreprises, compromettant ainsi la sécurité de leurs systèmes d'information.

Dans ce contexte, notre travail nous a permis dans un premier temps de maitre en valeurs la panoplie des solutions permettant d'assurer l'anonymat et le respect de la vie privée dans l'internet ainsi que les risques associés à leur utilisation. À ce titre, nous avons étudié en particulier l'emploi du réseau anonyme JonDonym dans un réseau d'entreprise, où nous avons démontré comment ce dernier permettait de passer outre les mesures de sécurité établies dans un LAN et de compromettre par conséquent sa sécurité.

Dans un second lieu, nous avons proposé une solution qui consiste à détecter l'usage de ce réseau anonyme (sur pc et smartphone) dans un réseau local. Cette détection se fait en plusieurs étapes : La première étape nous a permis de procéder à la capture avec le logiciel "Wireshark", des paquets transitant dans le réseau d'entreprise qui utilise le réseau JONDONYM et ce, pour extraire les informations nécessaires pour l'analyse.

Dans la phase analyse nous avons comparé les paquets capturés par les trois navigateurs Google Chrome, Firefox et Jondobrowser en utilisant l'analyseur de paquets DPI (Deep Packet Inspection) pour déceler l'empreinte numérique du réseau JonDonym. Ayant réussi avec succès à identifier cette empreinte, nous l'avons implémenté dans le système de détection d'intrusion IDS "Suricata" pour générer des alertes qui permettent

de signaler les menaces. Ainsi, la dernière phase a porté sur le test de la solution qui s'est étalé sur une période d'un mois durant lequel les alertes générées par « Suricata» étaient toutes valables. Il importe de signaler que les alertes les plus fréquentes concernaient les alertes de « Total Length » vu que la majorité des paquets avaient la même taille.

Enfin, faute de temps et de moyens, nous n'avons pas pu aller jusqu'au bout de notre solution qui visait à bloquer l'accès à internet à ces réseaux au sien d'un réseau d'entreprise. Pour cela nous pensons que notre travail pourrait constituer une bonne assise pour d'autres recherches plus avancées dans ce domaine.

Références

[1] https://radioalgerie.dz/news/fr/article/20200922/199644.html?fbclid=IwAR1bwwc5-QrOE8lk4fwzxSdFdefbaP3ODDggL05J17jmxzUYot0qz79mP54 , juin 2022

[2] BENJAMIN WALKER : 'COMPUTER NETWORKING', SCIENCE & TECHNOLOGY, 3 NOVEMBER 2019.

[3] John Wiley & Sons Inc: 'Networking All-in-One', Doug Lowe, 8th édition, 24 juin 2021.

[4] https://www.geeksforgeeks.org/what-is-internet-definition-uses-working-advantages-and-disadvantages/ , juin 2022

[5] http://www.assignmenthelp.net/assignment_help/intranet-extranet , juin 2022

[6] https://community.fs.com/blog/tcpip-vs-osi-whats-the-difference-between-the-two-models.html?fbclid=IwAR31Degk_o4jPaPbQh_8GuKfbKg_yAGOOyOxKi07H49tVPRvk1hvwtbbhyw , juin2022

[7]https://blog.eleven-labs.com/fr/comprendre-le-ssltls-partie-4-handshake-protocol/?fbclid=IwAR0B-6aXiPF8T2s2hZiTLN8xhRSrEGm5-f6nvodoc-DjKkh1wSpRrNtNCnY , juin 2022

[8] https://usemynotes.com/what-is-network-address-translation/ , juin 2022

[9] https://www.gns3network.com/what-is-nat/ , juin 2022

[10] https://data-flair.training/blogs/tcp-port/ , juin 2022

[11]https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa , juin 2022

[12] Craig Hunt : 'TCP/IP Network Administration, 3rd Edition', O'Reilly Media, April 2002

[13] https://www.actualidadgadget.com/dmz-host/ , juin 2022

[14]https://fr.sawakinome.com/articles/internet/unassigned-3856.html?fbclid=IwAR15VpyILsl1lUyZsECS__I_P6AUq6GTw13fZiMlnoHx24uRd6SVVl07NJ8 , juin 2022

[15] Walter Goralski : 'The Illustrated Network', ND édition

[16] https://privmx.com/blog/33/privacy-vs-anonymity , juin 2022

[17]https://www.investopedia.com/terms/d/dark-web.asp , juin 2022

[18] ISSUES IN INFORMATION SYSTEMS VOLUME 17, ISSUE IV, PP. 36-41, 2016

[19] STEVEN GATES : 'Réseau Anonyme TOR 101', BoD – BOOKS ON DEMAND.

[20] Daniel Echeverri Montoya :' Deep web : TOR, FreeNET & I2P Privacidad y Anonimato ', ZeroXword Computing.

[21] https://www.javatpoint.com/java-anon-proxy , juin 2022

[22] https://anon.inf.tu-dresden.de/index_en.html , juin 2022

[23] Milivoj Simeonovski : ' Accountable infrastructure and its impact on internet security and privacy', Universität des Saarlandes.

[24] https://anon.inf.tu-dresden.de/develop/doc/mix/index.html , juin 2022

[25] Synthèse AES 128, J.M. Dutertre – 2011

[26] https://www.geeksforgeeks.org/rsa-algorithm-cryptography/ , juin 2022

[27] DARK WEB CRIMES : https://www.findlaw.com/ , MAI 2022

[28] Research on Network Traffic Identification based on Machine Learning and Deep Packet Inspection, School of Information and Communication, National University of Defense Technology Wuhan, China.

[29] Adrian Yanes : 'Privacy and Anonymity', Aalto University- School of Electrical Engineering.

[30] JESSEY BULLOCK / JEFF T.PARKER : 'wireshark for security professionals', WILEY

[31] https://www.techno-science.net/glossaire-definition/Systeme-de-detection-d-intrusion.html , juin 2022

[32] AMALOU Warda & DELLAL Marwa : 'Elaboration d'une solution de détection du réseau anonyme Orbot', Université SAAD DAHLAB de BLIDA,2019/2020.

[33] Mohammed EL-Sayed GADELRAB, 'Évaluation des Systèmes de Détection d'Intrusion ', thèse de doctorat, université de TOULOUSE, France 15/12/2008

[34]https://net-security.fr/security/suricata-rules/?fbclid=IwAR1wFzNKO3fu8zRGpBubEpH9QUwTxIoWbb_huj7Zy_TG6Wp-e5TXuy7lRF8 , juin 2022

[35]https://suricata.readthedocs.io/en/latest/rules/intro.html?fbclid=IwAR2VZFNxD34Zg-QfykLqqERw-1BIG91l6J672OGXJvrOAS-T3cRby7cn1Y8 , juin 2002

[36] https://ipcisco.com/lesson/tcp-window-size-checksum-urgent-pointer/ , juin 2022