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

UNIVERSITE BLIDA 1
Faculté de Technologie
Département d'Électronique

MEMOIRE DE MASTER
En Télécommunication

Spécialité : Réseaux & Télécommunications
RT14

THÈME :

Mise en place d'une solution de supervision pour les réseaux VPN

Réalisée par
Ouadjina Khadidja Nada
Kerkab Hadir

Encadré par
Mr MEHDI Merouane

Juin 2025

Dédicace

C'est avec une profonde gratitude et des mots sincères que je dédie ce modeste travail de fin d'études à ma raison de vivre, à mes très chers parents. Merci de m'avoir toujours soutenue dans mes études, pour votre confiance, et surtout pour tout votre amour.

À ***mon père****, qui a sacrifié sa vie pour ma réussite, éclairé mon chemin par ses conseils avisés, sa patience sans limite, ses encouragements et son aide.*

À ***ma mère****, mon plus grand soutien dans les moments difficiles, toujours présente avec ses prières à chaque étape de mon parcours. Elle m'a donné tout l'amour et l'encouragement dont j'avais besoin. Merci maman, j'espère qu'un jour tu seras fière de moi.*

À mes frères ***Hichem*** *et* ***Abderrahim****, ainsi qu'à ma belle-sœur* ***Khadidja****, il m'est difficile d'exprimer en quelques mots toute la gratitude que je ressens envers vous. Merci pour votre amour sincère, votre présence rassurante et vos encouragements constants.*

À toute ma famille, merci d'avoir toujours cru en moi et de m'avoir entourée de tant d'affection.

À mes amies ***Mirine, Abir, Assia, Imène, Rihab*** *et* ***Nabila****, merci pour votre amitié, vos sourires et votre soutien indéfectible tout au long de ce parcours.*

Et une dédicace toute spéciale à mon binôme ***Kerkab Hadir****. Merci pour ton engagement, ta patience, ta rigueur et ta bonne humeur. Travailler avec toi a été une véritable chance. Ton professionnalisme, ton écoute et ta gentillesse ont fait de notre collaboration une expérience inoubliable. Je te suis sincèrement reconnaissante pour tout ce que nous avons partagé.*

Ouadjina Khadidja Nada

Dédicace

Avec tout honneur et fierté, je dédie ce modeste travail de fin d'études :

À la plus belle perle du monde, qui m'a donné la vie, la tendresse et les encouragements pour réussir... ***Ma tendre mère Maha****.*

celui qui a toujours été l'épaule solide, l'œil attentif, l'esprit compréhensif, et la personne la plus digne de mon estime et de mon respect... ***Mon cher père Nabil****.*

Les mots m'échappent et s'envolent, incapables de traduire mes sentiments pour vous.

Dieu seul pourra vous récompenser en vous accueillant dans Son paradis.

À mes précieux piliers de vie, ***mes sœurs Rimah et Amira****, ainsi que* ***mon frère Mustapha****, dont l'amour sincère, le soutien indéfectible et la présence apaisante ont été pour moi une source constante de force, de sérénité et d'inspiration..*

À toute ma famille, merci pour votre confiance constante et l'amour dont vous m'avez toujours entourée.

À tous mes amis, pour leur présence et leur soutien tout au long de ce parcours, je vous suis profondément reconnaissante. Et une pensée toute particulière à ***Imene, Rihab et Syrine*** *, dont l'amitié m'a portée avec une chaleur et une légèreté inoubliables. Vous êtes une richesse dans ma vie.*

Une dédicace spéciale à mon binôme, ***Ouadjina Khadidja Nada****. Ton soutien discret, ta patience et ta lumière dans les moments sombres ont illuminé ce chemin. Tu as été bien plus qu'une binôme, une présence rare et précieuse. Je te porte dans mon cœur avec une immense gratitude et une profonde affection.*

Kerkab Hadir

Remerciements

Nous tenons tout d'abord à exprimer notre gratitude à ALLAH le Tout-Puissant et Miséricordieux, qui nous a accordé la force, la patience et la persévérance nécessaires pour mener à bien ce modeste travail.

Nous exprimons ensuite notre profonde reconnaissance à **Mr Mehdi Merouane**, enseignant au département d'Électronique, spécialité Réseaux et Télécommunications, pour son encadrement précieux, sa disponibilité constante, ses conseils avisés et sa confiance tout au long de notre parcours et particulièrement lors de la réalisation de ce projet. Son accompagnement a été déterminant pour aboutir à ce résultat.

Nous souhaitons également adresser nos sincères remerciements aux membres du jury pour l'honneur qu'ils nous font en évaluant ce travail, ainsi que pour l'intérêt qu'ils y portent.

Un grand merci à nos familles, dont le soutien indéfectible, les encouragements et l'appui moral ont été une source précieuse de motivation et de sérénité tout au long de cette aventure.

Enfin, nous adressons notre reconnaissance à toutes les personnes qui, de près ou de loin, nous ont apporté leur aide, leur soutien ou leurs encouragements dans l'accomplissement de ce travail.

ملخص

تُعدّ مراقبة الشبكات الافتراضية الخاصة (فبن) داخل الشركات مسألة بالغة الأهمية نظرًا لتعقيد البنى التحتية للشبكات ووجود تهديدات محتملة. وفي هذا الإطار، قمنا بتطوير حلّ لمراقبة شبكات فبن يعتمد على هيكلية عميل-خادم. لقد قمنا بمحاكاة أنشطة مشبوهة على شبكة فبن، مثل تجاوز البروكسي، والاتصالات غير المصرّح بها، ونقل البيانات غير المعتاد. وبفضل أدوات اوبيماناجر و بيرتيجي، تمكّنا من مراقبة أداء شبكة الـفبن في الوقت الحقيقي، واكتشاف الشذوذ، وضمان توفر الاتصالات عن بُعد. وقد مكّنتنا هذه الأدوات من تحليل فعّال واستجابة سريعة تجاه الحوادث.

الكلمات المفتاحية: شبكة افتراضية خاصة، مراقبة، بروكسي، اوبيماناجر، بيرتيجي.

Abstract

VPN monitoring within enterprises is a major challenge due to the increased complexity of network infrastructures and potential threats. To this end, we developed a VPN monitoring solution based on a client-server architecture. We replicated suspicious activities on the VPN network, such as proxy bypasses, unauthorized connections, and unusual data transfers. Thanks to OpManager and PRTG, we were able to monitor VPN performance in real time, detect anomalies, and ensure the availability of remote connections. These tools enabled efficient analysis and rapid response to incidents.

Keywords: VPN, monitoring, proxy, OpMnager, PRTG.

Résumé

La supervision des réseaux VPN au sein des entreprises constitue un enjeu majeur en raison de la complexité accrue des infrastructures réseau et des menaces potentielles. Dans ce cadre, nous avons développé une solution de monitoring des réseaux VPN reposant sur une architecture client-serveur. Nous avons reproduit des activités suspectes sur le réseau VPN, telles que des contournements de proxy, des connexions non autorisées et des transferts de données inhabituels. Grâce à OpManager et PRTG, nous avons pu surveiller en temps réel les performances du VPN, détecter les anomalies et assurer la disponibilité des connexions distantes. Ces outils ont permis une analyse efficace et une réaction rapide face aux incidents.

Mots Clée : VPN, surveillance, proxy, OpMnager, PRTG.

Liste des Acronymes et Abréviations

3COM 3Computer Communication Compatibility

ACL Access Control Lists

AES Advanced Encryption Standard

AG Aktiengesellschaft

AH Authentication Header

CPU Central Processing Unit

DNS Domain Name System

ESP Encapsulating Security Payload

GRE Generic Routing Encapsulation

GPL General Public License

HIDS Host-Based Intrusion Detection System

HTTP HyperText Transfer Protocol

HTTPS HyperText Transfer Protocol Secure

ICMP Internet Control Message Protocol

IDS Intrusion Detection System

IETF Internet Engineering Task Force

IOT Internet of Things

IP Internet Protocol

IPMI Intelligent Platform Management Interface

IPSEC Internet Protocol Security

IPS Intrusion Prevention System

IPX Internetwork Packet Exchange

IT Information Technology

JMX Java Management Extensions

LAN Local Area Network

L2TP Layer 2 Tunneling Protocol

MAC Media Access Control

NDSS Network and Distributed System Security

PC Personal Computer

PME Petite et Moyenne Entreprise

PPP Point-to-Point Protocol

PPTP Point-to-Point Tunneling Protocol

PRTG Paessler Router Traffic Grapher

P2P Peer-to-Peer

SIEM Security Information and Event Management

SLIP Serial Line Internet Protocol

SMS Short Message Service

SNMP Simple Network Management Protocol

SSL Secure Sockets Layer

TLS Transport Layer Security

URL Uniform Resource Locator

US Robotics United States Robotics

VOIP Voice Over Internet Protocol

VPN Virtual Private Network

VMware Virtual Machine ware

WAN Wide Area Network

WEB World Wide Web

WMI Windows Management Instrumentation

WI-FI Wireless Fidelity

XDR Extended Detection and Response

Table des matières

Table des figures

Liste des tableaux

Introduction Générale

De nos jours, La sécurité des systèmes d'information est un enjeu crucial pour toute organisation évoluant dans un environnement numérique. Face à la croissance exponentielle des cybermenaces telles que les fuites de données sensibles, l'espionnage industriel ou encore les attaques par déni de service, il est devenu impératif de mettre en place des mécanismes de protection efficaces pour assurer la confidentialité, l'intégrité et la disponibilité des informations.

La technologie VPN a été mise en place pour contrer ce problème de sécurité et assurer la protection des communications sur des réseaux publics. Le VPN est largement adopté dans les contextes professionnels pour le télétravail, l'accès sécurisé aux ressources internes, ou encore la protection contre la surveillance en ligne.

Néanmoins, l'efficacité d'une solution VPN ne se limite pas à son déploiement, mais nécessite également une surveillance continue et proactive. La surveillance des systèmes informatiques et des réseaux est devenue une exigence essentielle pour assurer la sécurité, la performance et la continuité des activités. Elle permet de superviser en temps réel les infrastructures critiques, de détecter rapidement les anomalies ou intrusions, et de prévenir les interruptions de service. Grâce à des outils spécialisés de surveillance et de supervision, il est aujourd'hui possible de suivre en temps réel plusieurs aspects du fonctionnement réseau, tels que le trafic, la disponibilité des équipements, et les performances globales du système.

À partir de ces constats, ce mémoire s'intéresse à la problématique suivante : Comment mettre en place une solution VPN fiable et sécurisée, tout en assurant sa surveillance afin de garantir un usage conforme et optimal dans un environnement professionnel ?

Le but de cette étude est de concevoir et déployer une solution VPN qui soit à la fois fiable, sécurisée et efficacement supervisée, répondant aux exigences d'un environnement professionnel. Cela inclut non seulement la mise en place technique du VPN, notamment avec OpenVPN et HolaVPN, mais également l'intégration d'outils de supervision en temps réel afin d'assurer la disponibilité du service, la confidentialité des échanges et des performances optimales du système. L'étude vise à :

— Garantir un accès sécurisé aux ressources internes via un VPN professionnel.
— Déployer une surveillance réseau capable de détecter anomalies et intrusions.
— Évaluer l'efficacité du VPN face aux tentatives de contournement.
— Évaluer l'apport d'OpManager et PRTG dans le suivi et la détection d'incidents.

Le mémoire abordera dans le premier chapitre une présentation approfondie des réseaux VPN.

Le deuxième chapitre présentera en détail la mise en œuvre de la solution de surveillance VPN. Nous commencerons par l'utilisation d'une architecture proxy pour restreindre l'accès à certains sites, avant de tester leur contournement à l'aide de logiciels VPN, mettant ainsi en évidence leur efficacité et leurs limites. Enfin, nous aborderons l'installation et la configuration des outils de supervision réseau, tel que OpManager et PRTG.

Le troisième chapitre sera dédié à l'évaluation de la solution déployée. Il présentera les résultats des tests réalisés, analysera les données collectées par les outils de supervision, et mettra en lumière les observations concernant la performance et l'efficacité du système mis en place.

Enfin, nous terminons par une conclusion générale.

Chapitre 1

Généralité sur les réseaux VPN

1.1 Introduction

À l'ère du numérique, Internet est l'épine dorsale de la connectivité mondiale, transformant nos modes de vie, de travail et de communication. Cependant, son développement s'accompagne de défis majeurs en matière de sécurité, notamment avec l'explosion du nombre d'appareils IoT, qui devrait atteindre 75 milliards dans un avenir proche, un chiffre qui ne fera qu'augmenter, et avec lui, les problèmes.

La sécurité est un aspect essentiel de nos vies, mais Internet présente d'importantes vulnérabilités. Par concequence, nos données personnelles sont exposées à des risques d'accès non autorisés, ce qui souligne la nécessité de remédier à ces incertitudes. [11]

Dans ce contexte, les réseaux privés virtuels (VPN) jouent un rôle crucial en offrant une solution pour sécuriser les communications sur Internet. Un réseau privé désigne un ensemble restreint de membres autorisés ayant un accès exclusif aux services et ressources disponibles, ou les données circulant au sein d'un réseau privé restent confinées et protégées contre les interférences avec le trafic externe. [12]

1.2 Présentation des VPN

1.2.1 Définition

Un réseau privé virtuel (VPN) est une infrastructure virtuelle qui exploite un réseau public pour établir des connexions sécurisées entre ses nœuds. Il permet l'échange de données confidentielles via un réseau public, sans nécessiter de liaison physique directe entre les points de communication. Cette solution constitue une alternative économique aux infrastructures physiques, en tirant parti de réseaux publics comme Internet pour

assurer des communications sécurisées à moindre coût. [13, 14]

VPN est une technologie conçue pour renforcer l'anonymat et la sécurité en ligne d'un utilisateur, notamment en masquant sa localisation et en protégeant son activité sur Internet. Il établit une connexion virtuelle de type point à point, s'appuyant sur le chiffrement et d'autres protocoles sécurisés afin de préserver la confidentialité des données transmises sur un réseau traditionnel. [15]

1.2.2 Principe de fonctionnement

Le VPN repose sur un protocole de tunneling, qui permet de chiffrer les données en utilisant un algorithme cryptographique entre deux réseaux.

Ce protocole de tunnelisation crée un canal virtuel entre un émetteur et un destinataire une fois qu'ils sont identifiés. Ensuite, la source chiffre les données et les transmet via ce canal sécurisé. Les VPN reproduisent ainsi le fonctionnement d'un réseau privé tout en s'appuyant sur une infrastructure partagée comme Internet.

Le tunneling est un procédé qui consiste à encapsuler, transmettre, puis décapsuler des données. Lorsqu'un protocole autre que l'IP est utilisé pour la transmission, le protocole de tunneling ajoute un en-tête aux données afin de les encapsuler. Ce mécanisme permet de transporter différents types de protocoles tout en assurant la sécurité des échanges. Ainsi, les VPN peuvent fournir un accès fiable, simple et économique aux intranets ou extranets d'entreprise, tout en protégeant les données contre toute interception non autorisée. [16]

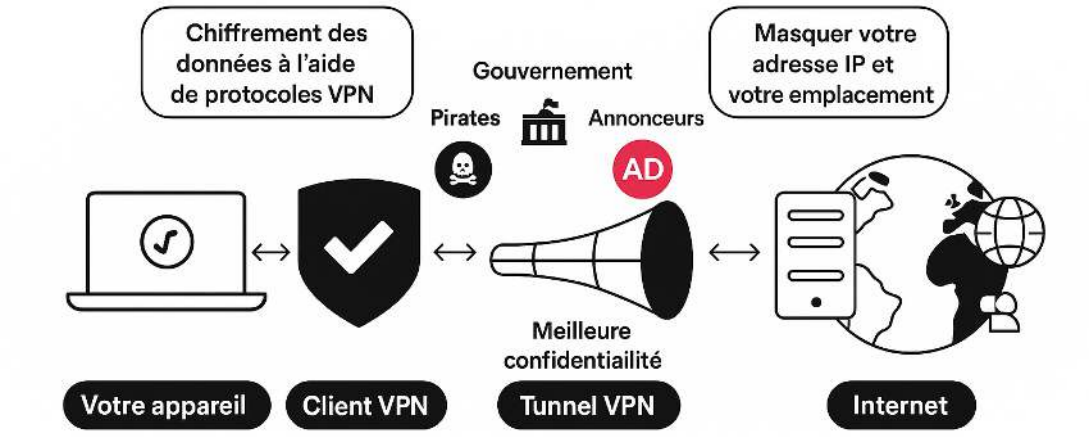

Figure 1.1 – Schéma de fonctionnement de vpn [1]

1.3 Les Protocoles VPN

1.3.1 Le protocole PPP (Point-To-Point Protocol)

C'est un ensemble de protocoles standard garantissant l'interopérabilité des logiciels d'accès distant de divers éditeurs, il permet de transférer des données sur un lien synchrone ou asynchrone, il est full duplex, garantie l'ordre d'arrivée des paquets et encapsuler les paquets IP, IPX dans des trames PPP, puis transmet ces paquets encapsules au travers de liaison point à point. [17]

1.3.2 Le protocole PPTP (Point-to-Point Tunneling Protocol)

Est un protocole de niveau 2 développé par Microsoft, 3Com, Ascend, US Robotics .

Le protocole de tunneling point à point est un protocole permettant de stocker les données et de créer un tunnel. Grâce à la connexion Internet actuelle, les utilisateurs distants peuvent se connecter à un réseau VPN via des VPN PPTP. Cela est avantageux pour les particuliers et les professionnels. L'accès au VPN nécessite une connexion avec un mot de passe approuvé. Le VPN PPTP est le VPN le plus couramment utilisé, car il est compatible avec des systèmes d'exploitation tels que Windows, Linux et Mac. Malgré ses avantages, ce type de VPN présente également des inconvénients, notamment l'absence de chiffrement, ce qui n'est pas idéal pour les entreprises, dont l'objectif principal est d'assurer la sécurité des données. [18]

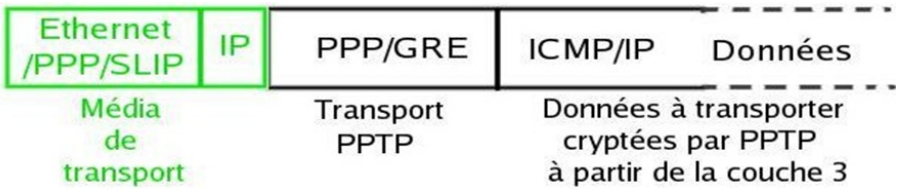

Figure 1.2 – Packet de connexion PPTP [2]

1.3.3 Le protocole IPSEC (Internet Protocol Security)

Est un protocole de niveau 3, issu des travaux de l'IETF, permettant de transporter des données chiffrées pour les réseaux IP.

IPSEC est une suite de protocoles normalisés conçue pour sécuriser les communications VPN. Il renforce la sécurité du trafic IP, il est basé sur deux mécanismes :

Le premier AH (Authentification Header) permet d'assurer l'intégrité et l'authenticité des datagrammes IP.

Le second ESP (Encapsulating Security Payload) peut aussi permettre l'authentification des données mais il est principalement utilisé pour le cryptage des informations. Grâce à ses mécanismes de sécurité avancés, Ipsec facilite l'établissement de tunnels VPN hautement sécurisés. [19]

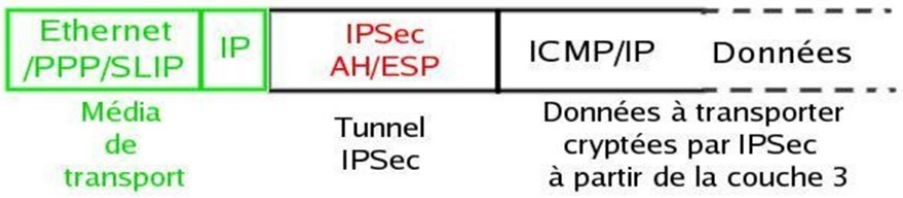

FIGURE 1.3 – Packet de connexion IPSEC [2]

1.3.4 Le protocole L2TP (Layer Two Tunneling Protocol)

Est l'aboutissement des travaux de l'IETF (RFC 2661) pour faire converger les fonctionnalités de PPTP. Il s'agit ainsi d'un protocole de niveau 2 s'appuyant sur PPP.

L2TP permet d'établir un canal de communication sécurisé au sein d'un réseau non sécurisé. Il est généralement couplé à un protocole tel qu'Ipsec pour renforcer la sécurité. Son objectif principal est d'assurer la transmission chiffrée de données encapsulées entre deux nœuds d'un réseau privé virtuel (VPN) Les protocoles d'authentification utilisés pour établir des tunnels L2TP sont les mêmes que ceux employés par le protocole PPTP, hérités du protocole PPP. Étant donné que L2TP, pris seul, n'offre pas de sécurité suffisante, il est fréquemment associé à d'autres protocoles comme IPSec, OpenVPN et WireGuard pour en renforcer la protection. [12]

1.3.5 Le protocole OpenVPN

Le Protocole Open VPN est une application informatique ouverte pour la mise en place de techniques de réseaux privés virtuels, avec des connexions sécurisées point-par-point ou site-par-site, pour des configurations via routage ou pont, ainsi que pour les accès à distance. Il exploite un protocole de sécurité sur mesure qui utilise SSL/TLS pour les échanges clés.

Un protocole Open VPN permet à des homologues de s'authentifier mutuellement en utilisant une clé secrète pré-partagée, des certificats ou un nom d'utilisateur / mot de passe. Lorsqu'il est utilisé dans une configuration multi client-serveur, il permet au serveur de libérer un certificat d'authentification pour chaque client, en utilisant la signature et l'autorité de certification. Ce système utilise en grande partie la base de cryptage

OpenSSL, ainsi que le protocole SSLv3/TLSv1 et contient de nombreuses fonctionnalités de sécurité et de contrôle.

1.3.6 Le protocole SSL/TLS

Le protocole SSL, quant à lui, utilise les protocoles SSL (Secure Sockets Layer) ou TLS (Transport Layer Security) pour sécuriser la transmission des données. Il fonctionne au niveau de la couche applicative (couche 7), généralement via un navigateur web standard, et ne nécessite aucun logiciel client spécifique. Les VPN SSL sont souvent utilisés pour l'accès à distance à des applications spécifiques ou à des services web. Plus faciles à déployer et plus conviviaux, ils constituent un excellent choix pour les utilisateurs individuels ou les organisations ayant besoin d'accéder à des applications web internes. [20]

1.3.7 Le protocole WireGuard

WireGuard (Donenfeld, NDSS 2017) est un tunnel réseau sécurisé récemment proposé, fonctionnant au niveau de la couche 3. WireGuard vise à remplacer les solutions de tunneling existantes comme IPsec et OpenVPN, tout en nécessitant moins de code, en étant plus sûr, plus performant et plus simple d'utilisation. [21]

1.4 Les types de VPN

Une organisation a le choix entre plusieurs types de VPN selon l'entité avec laquelle elle veut être interconnectée.

1.4.1 VPN d'accés (Host to LAN)

Les VPN d'accés à distance offrent aux utilisateurs éloignes la possibilité de se connecter à leur réseau local prive tout en préservant la confidentialité grâce à une infrastructure de réseau public. [22] Cela permet aux employés à domicile ou mobiles/à distance d'accéder au réseau interne de l'entreprise et d'utiliser leurs services et ressources en exploitant l'infrastructure des réseaux publics, comme Internet. [23, 24]

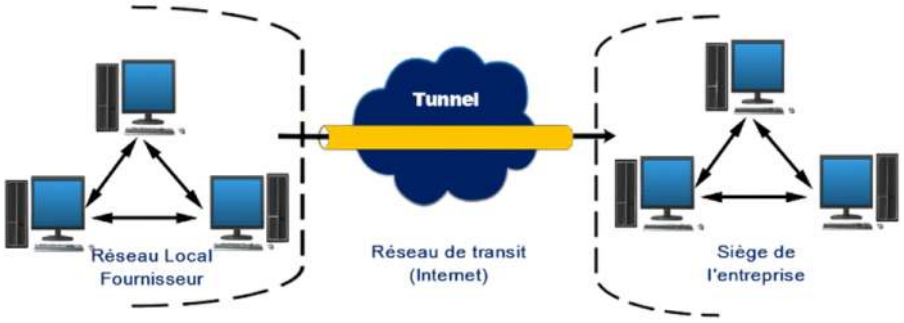

FIGURE 1.4 – Schéma de type HOST to LAN. [3]

1.4.2 Intranet VPN (LAN to LAN)

Le VPN site à site, aussi appelée tunnel VPN routeur-routeur, permet une connexion sécurisée entre plusieurs utilisateurs situés à des emplacements fixes [25, 26]. Il est particulièrement adapté aux organisations, car il leur permet d'établir une connexion sécurisée entre leurs sites géographiquement dispersés via le réseau public. [25]

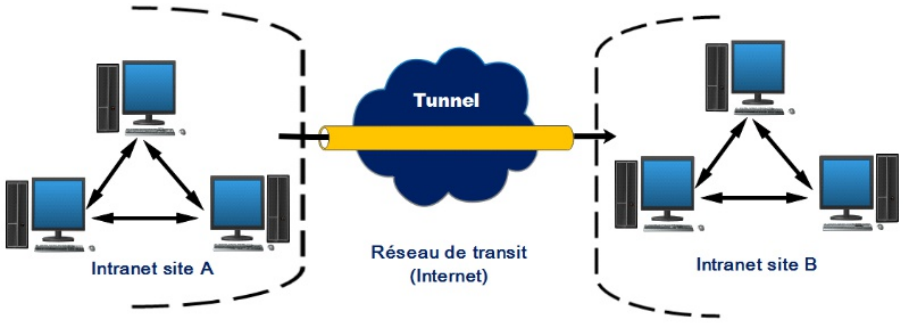

FIGURE 1.5 – Schéma de type LAN to LAN. [3]

1.4.3 Extranet VPN (Host to Host)

Le VPN poste à poste est utilisé pour connecter deux ordinateurs distants entre eux pour des raisons de confidentialité. On crée donc un VPN entre eux, et toutes les données y transmises sont encryptées et compréhensibles que par les deux paires correspondantes. Ce type de VPN est utilisé par les entreprises afin de communiquer avec ses clients en ouvrant son réseau local à ses clients ou partenaires. [27]

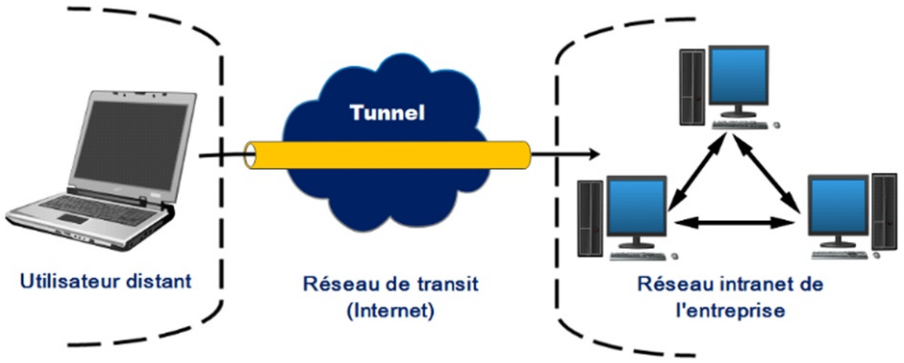

FIGURE 1.6 – Schéma de type HOST to HOST. [3]

1.5 Les avantage et les inconvénients des VPNs

1. **Les avantages :**
   - Intimité et sécurité améliorées.
   - Protection contre les pirates et les cybermenaces.
   - Navigation sécurisée sur les réseaux Wi-Fi publics.
   - Éviter la collecte de données.
   - Sécurisation des achats et transactions bancaires en ligne.
   - Gestion des accès sécurises pour le travail à distance.
2. **Les inconvénients :**
   - Réduction de la vitesse de connexion.
   - Compatibilité avec certains services.
   - Complexité d'utilisation.
   - Utilisation illégale dans certains pays.
   - Utilisation d'un VPN avec des services de VoIP.
   - Risques liés aux VPN peu fiables.

1.6 Les menaces et les risques liés aux VPN

Les VPN (Réseaux Privés Virtuels) sont des outils puissants pour protéger la vie privée et la sécurité en ligne, mais ils comportent également des menaces et des risques potentiels. Voici quelques-uns des principaux risques associés aux VPN :

1. **Fuites DNS et IP**
   - Fuites DNS : Les requêtes DNS peuvent ne pas être routées via le tunnel VPN, exposant ainsi les activités de navigation à des tiers. [28]

— Fuites IP : L'adresse IP réelle peut être divulguée, compromettant l'anonymat et la confidentialité. [28]

2. **Attaques par Force Brute et Vulnérabilités des Protocoles**
   — Les attaques par force brute ciblent les serveurs VPN pour deviner les identifiants ou les clés de chiffrement. [28]
   — Certains protocoles VPN, comme PPTP, sont moins sécurisés et peuvent être exploités par des attaquants. [28]
3. **Utilisation par les Hackers**
   — Les hackers utilisent les VPN pour masquer leur identité et localisation, rendant difficile la traçabilité de leurs activités illicites. [29]
4. **Risques liés aux VPN Gratuits**
   — Collecte de Données : Les VPN gratuits peuvent collecter et vendre des données personnelles pour financer leurs activités. [30]
   — Failles de Sécurité : Ils utilisent souvent des protocoles de chiffrement faibles, laissant les utilisateurs vulnérables aux cyberattaques. [30, 31]
   — Publicités Intrusives et Malwares : Ils peuvent intégrer des publicités indésirables et des malwares, compromettant la sécurité des appareils. [26, 30]

1.7 Enjeux et défis de la supervision des VPN

1.7.1 La surveillance des réseaux VPNs

La surveillance des connexions VPN constitue un enjeu stratégique majeur pour la sécurité des systèmes d'information. Grâce à un suivi en temps réel des tunnels VPN, les administrateurs sont en mesure d'identifier rapidement des anomalies telles que des coupures de service, des ralentissements ou des tentatives d'accès non autorisées. La surveillance est essentielle pour plusieurs raisons stratégiques tels que :

1. **Sécurité renforcée**
   — S'assurer que le trafic reste bien chiffré afin de prévenir toute fuite de données sensibles.
   — Détecter les tentatives d'accès non autorisées et les connexions problématiques de comptes obsolètes, notamment les risques d'intrusion. [32]
2. **Optimisation des performances**
   — Identifier les problèmes de latence ou de perte de paquets qui peuvent impacter la productivité des utilisateurs. [32, 33]

— Analyser l'utilisation de la bande passante afin d'optimiser la répartition des ressources réseau.

3. **Conformité aux règlementations**
   — Auditer et tracer les connexions VPN pour répondre aux exigences des normes de sécurité et de protection des données.
4. **Gestion des accès**
   — Suivre les sessions actives (SSL, IPsec) et contrôler les utilisateurs connectés afin de limiter les menaces internes et éviter les abus d'accès.

1.7.2 Les méthodes de surveillances

1. **Journalisation des connexions**
   — Enregistrement des données : les heures de connexion/déconnexion, les adresses IP utilisées, la bande passante consommée, etc.
   — Objectif : Suivre l'utilisation du VPN par les utilisateurs et d'identifier des comportements inhabituels.
2. **Analyse du trafic réseau**
   — Surveillance du trafic : volume et le type de trafic qui transite par le VPN.
   — Objectif : Détecter des pics de données suspects, du trafic non autorisé ou des tentatives d'exfiltration de donnée
3. **Détection d'anomalies et alertes (IDS/IPS)**
   — Outils utilises : Des systèmes comme Snort, Suricata.
   — Objectif : Configurés ces systèmes pour détecter des comportements inhabituels sur le VPN.
4. **Surveillance des authentifications**
   — Objectif : Repérer des tentatives de brute-force, des connexions multiples suspectes, ou l'usage de comptes compromis.
5. **Contrôle via pare-feu ou proxy**
   — Utilisation : Firewalls de nouvelle génération pour filtrer et inspecter le trafic VPN.
   — Objectif : Bloquer certains protocoles VPN non autorisés (PPTP, L2TP, etc.).
6. **Protocole ICMP**
   — Utilisation : Vérifier le chemin des données IPsec et détecter les problèmes de connectivité.

1.7.3 Les outils de monitoring

Dans un environnement informatique où l'accès distant aux ressources internes devient de plus en plus courant, notamment avec l'essor du télétravail, la surveillance des connexions VPN s'avère indispensable. Elle permet de contrôler non seulement la disponibilité des tunnels sécurisés, mais aussi la qualité des connexions, le volume de trafic échangé, ainsi que les tentatives de connexion suspectes, tels que :

1.7.3.1 OpManager

OpManager est une solution complète de gestion réseau, conçue pour superviser des environnements informatiques hétérogènes et multi-constructeurs. Il propose une approche unifiée pour le pilotage et l'évolution de l'infrastructure IT distribuée. Grace a ses fonctionnalités avancées, OpManager assure la surveillance des pannes et des performances sur l'ensemble des ressources critique du système d'information : équipements réseau, liaisons WAN ou VOIP, serveurs physiques et virtuels, ainsi que des applications clés comme Microsoft Exchange ou SQL server. [34]

Figure 1.7 – Logo OpManager. [4]

1.7.3.2 PRTG

PRTG Network Monitor est un logiciel de supervision réseau développé par l'entreprise Paessler AG. Il permet de surveiller en temps réel l'état et les performances des équipements informatiques, comme les serveurs, routeurs, commutateurs, bases de données, et autres appareils connectés au réseau. Grâce à des capteurs prédéfinis ou personnalisés, PRTG collecte des données sur la bande passante, l'utilisation du CPU, la mémoire, le trafic réseau, et alerte les administrateurs en cas d'anomalie. Il est largement utilisé pour anticiper les pannes, optimiser les performances et assurer la disponibilité des services informatiques. [35]

FIGURE 1.8 – Logo PRTG. [5]

1.7.3.3 NAGIOS

Nagios est un logiciel libre de supervision, distribué sous licence GPL, créé en 1999 par Ethan Galstad sous le nom initial de NetSaint. Il s'impose aujourd'hui comme l'une des solutions open source de supervision les plus connues et les plus largement utilisées. Nagios permet la surveillance en temps réel des systèmes et des réseaux, la détection rapide des incidents, ainsi qu'une supervision à l'aide d'agents. Il propose également un tableau de bord centralisé et constitue une solution fiable et sécurisée. [36]

FIGURE 1.9 – Logo NAGIOS. [6]

1.7.3.4 ZABBIX

Zabbix est un logiciel open source de supervision conçu pour surveiller en temps réel les performances et la disponibilité des équipements réseau, des serveurs, des machines virtuelles, des applications et des services. Il permet la collecte, l'analyse et la visualisation des données à travers une interface web centralisée. Grâce à son système d'alertes configurable, Zabbix facilite la détection proactive des incidents et l'automatisation des réponses. Il prend en charge divers protocoles tels que SNMP, IPMI, JMX, et propose aussi une supervision avec ou sans agents, s'adaptant ainsi à différents environnements informatiques. [37]

FIGURE 1.10 – Logo ZABBIX. [7]

1.7.3.5 WAZUH

Wazuh est une plateforme open-source de sécurité informatique qui combine les fonctionnalités d'un Host-based Intrusion system (HIDS) d'un Security Information and Event Managment (SIEM)et d'un eXtended Detection and REsponse (XDR). Il est conçu pour collecter et analyser des données de sécurité à partir de diverses sources, telles que des journaux d'événements et des données de trafic réseau, afin de détecter les menaces potentielles et générer des alertes en temps réel. Wazuh est également capable de surveiller l'intégrité des fichiers et de détecter les vulnérabilités, tout en offrant une vue centralisée pour la gestion des menaces. [38]

FIGURE 1.11 – Logo WAZUH. [8]

1.7.4 Analyse du trafic VPN et détection d'anomalies

L'analyse du trafic VPN devient un enjeu essentiel pour garantir la sécurité et la performance des infrastructures informatiques. L'analyse permet d'observer :

— Disponibilités et performances : Permet de vérifier si les tunnels VPN sont disponibles et fonctionnent correctement, en surveillants des indicateurs tels que la latence et la perte de paquets

— Sécurité : L'analyse du trafic aide à détecter les anomalies o les activités suspects, comme des tentatives d'intrusion ou des fuites de données, en utilisant des outils

de supervision et des techniques d'analyse comportementale.

— Optimisation des ressources : En identifiant les principaux utilisateurs de la bande passante, les organisations peuvent allouer efficacement les ressources réseau et optimiser les performances globales.

La détection d'anomalies est un élément clé dans la sécurité des réseaux VPN. Elle vise à identifier des comportements suspects ou inhabituels dans le trafic VPN, susceptibles de révéler une tentative d'intrusion, une fuite de données, un usage non autorisé du réseau ou encore une mauvaise configuration. Parmi les anomalies courantes, on peut citer :

— Des pics inattendus dans l'utilisation de la bande passante : Peuvent indiquer une surcharge inhabituelle ou une fuite de données.

— Des connexions provenant de sources inconnues : Souvent synonymes d'accès non autorisé ou d'intrusion.

— Des modèles de trafic atypiques : Peuvent signaler des activités malveillantes ou une mauvaise configuration du réseau.

C'est dans ce cadre que nous avons mis en œuvre une solution de surveillance spécialisée, conçue pour optimiser la gestion des VPN tout en garantissant une supervision efficace de leur utilisation et de leurs performances.

1.8 Conclusion

Au cours de ce chapitre, nous avons parcouru comment les VPN permettent de sécuriser les communications sur des réseaux publics. Nous avons aussi mis en évidence leurs limites et l'importance de leur supervision des VPN, à travers des outils de monitoring et de détection d'anomalies, afin de garantir un niveau de sécurité optimal et de prévenir les menaces potentielles.

Ces connaissances théoriques nous permettent d'aborder le chapitre suivant, qui sera consacré à la mise en œuvre pratique de la solution VPN. Nous y détaillerons l'installation des logiciels nécessaires, la configuration du réseau, la conception de l'architecture adoptée, ainsi que la mise en place des outils de surveillance.

Chapitre 2

Mise en place de l'architecture VPN

2.1 Introduction

Après avoir exploré les concepts fondamentaux liés aux VPN, ce chapitre se concentre sur la mise en place d'une architecture VPN fonctionnelle. Celle-ci vise à permettre aux utilisateurs distants d'accéder de manière sécurisée au réseau privé de l'entreprise et de garantir l'échange de données sensibles à travers un tunnel chiffré.

Nous aborderons également les aspects liés à la supervision de cette infrastructure, afin d'assurer un suivi constant des connexions, de détecter d'éventuelles anomalies et de maintenir un haut niveau de sécurité et de performance.

2.2 L'architecture de travail

Dans le cadre de notre architecture VPN, nous avons d'abord connecté le PC serveur à Internet, puis partagé cette connexion automatiquement avec le PC client via un câble RJ45. Pour gérer et sécuriser l'accès Internet, nous avons installé SQUID Proxy sur le serveur. Une fois la connexion VPN établie, tout le trafic Internet du client transite par ce proxy, ce qui permet d'appliquer des règles de filtrage avancées, notamment le blocage de sites web spécifiques. Afin d'assurer un suivi constant de l'activité réseau et de garantir l'intégrité de la connexion VPN, nous avons également mis en place une solution de surveillance permettant de superviser le fonctionnement du VPN, de détecter les anomalies et d'analyser les flux de données en temps réel. Voici les étapes suivie :

- La préparation d'environnement du travail avec les equipements nécessaires.
- Partage de connexion entre les postes.
- Configuration des adresses IP.
- Installation et configuration du squid.

- Installation des logiciels VPN client.
- Installation des logiciels de surveillance.

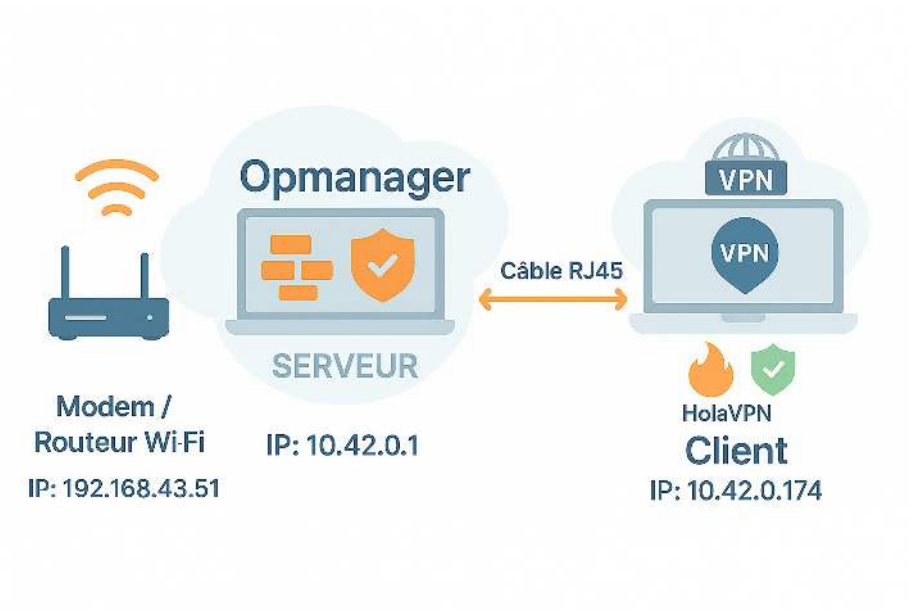

FIGURE 2.1 – Schéma de notre travail

2.3 L'environnement de travail

Au cours de la réalisation de notre architecture pour simuler un réseau d'entreprise, nous avons utilisé deux ordinateurs portables fonctionnant sous le système d'exploitation Windows et Linux.

2.3.1 Pour le serveur

Nous avons utilisé un PC Dell fonctionnant sous le système d'exploitation Linux, dont les caractéristiques sont présentées dans le tableau suivant :

Caractéristique	Détails
Nom de l'appareil	DESKTOP-IL6N7PF
Processeur	Intel(R) Core(TM) i7-10610U CPU @ 1.80GHz
RAM totale	15GiB
Architecture	x86_64
Système d'exploitation	Kali GNU/Linux Rolling
Espace disque total	268G

TABLEAU 2.1 – Caractéristiques du PC (serveur)

2.3.2 Pour le client

Nous avons eu recours à un ordinateur Lenovo équipé du système d'exploitation Windows, avec les caractéristiques suivantes :

Caractéristique	Détails
Nom de l'appareil	DESKTOP-2NPF8UT
Processeur	Intel Core i7-6600U CPU @ 2.60GHz-2.81GHz
RAM	8 Go
Type de système	64 bits
Système d'exploitation	Windows 10 Professionnel

Tableau 2.2 – Caractéristiques du PC (client)

Les deux machines ont été connectées directement à l'aide d'un câble RJ45, formant ainsi un réseau local simple entre le serveur et le client.

2.4 Mise en œuvre de l'architecture réseau

Voici les différentes étapes que nous avons suivies pour déployer l'architecture :

2.4.1 La préparation d'environnement du travail

Cette architecture reflète une mise en place réelle effectuée au cours de notre projet (**figure 2.2**).

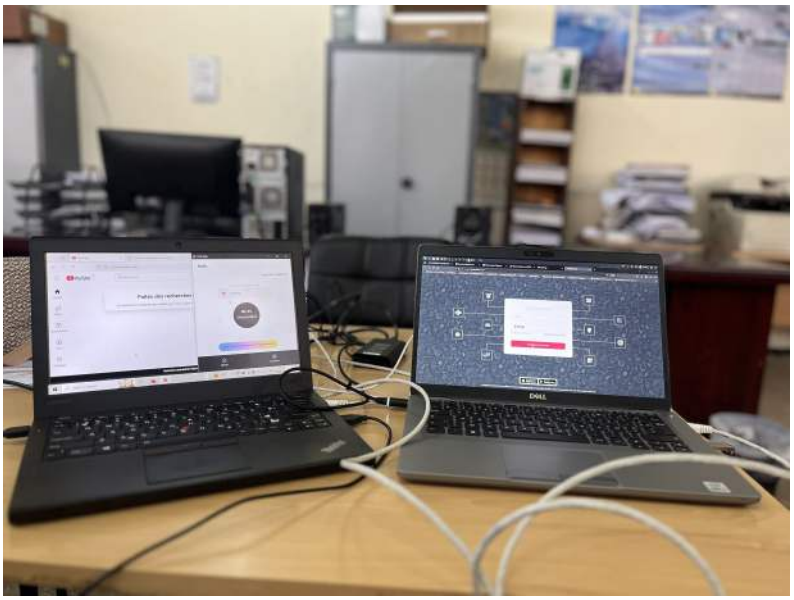

Figure 2.2 – Architecture de travail

2.4.2 Configuration des adresses IP

Une fois les PC prêtes, nous avons configuré leurs adresses IP de manière à permettre une communication directe entre le client et le serveur au sein du réseau local.

Afin d'assurer une disponibilité continue des services, une adresse IP statique a été attribuée au serveur.

2.4.2.1 Modification de l'adresse IP sous Linux (Serveur)

La configuration d'une adresse IP sous Linux peut se faire temporairement ou de façon permanente. Voici les étapes suivies pour modifier l'adresse IP de l'interface `eth0`.

— **Étape 1 : Identifier l'interface réseau**

Avant de procéder à la configuration, il convient de vérifier le nom de l'interface réseau :

```
ip a
```

Dans notre cas, l'interface utilisée est `eth0`.

— **Étape 2 : Configuration temporaire**

La commande suivante permet d'attribuer une adresse IP à l'interface `eth0` de manière temporaire (elle sera perdue après redémarrage) :

```
sudo ip addr flush dev eth0
sudo ip addr add 10.42.0.1/24 dev eth0
```

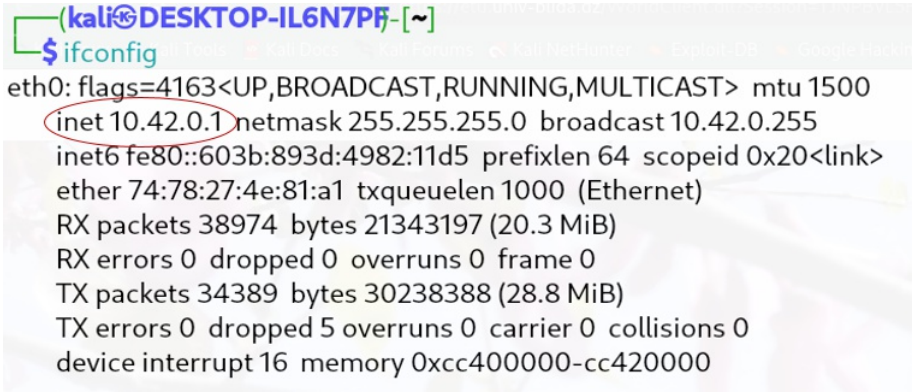

Figure 2.3 – Affichage add ip Côté serveur

2.4.2.2 Modification de l'adresse IP sous windows (Client)

Du côté client, une adresse IP appartenant au même sous-réseau a été configurée afin d'assurer la compatibilité avec le serveur, comme illustré dans la figure 2.4.

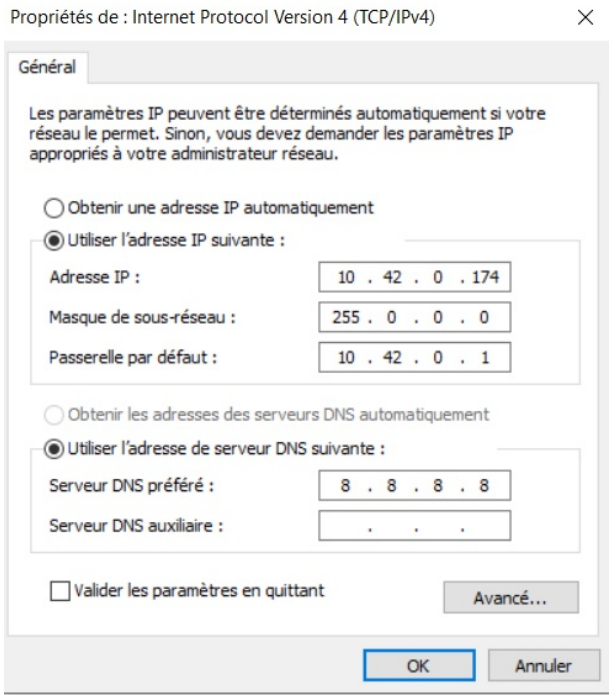

FIGURE 2.4 – Affichage add ip Côté client

Le PC utilise une connexion filaire grâce à un câble Ethernet, garantissant une liaison réseau stable et rapide.

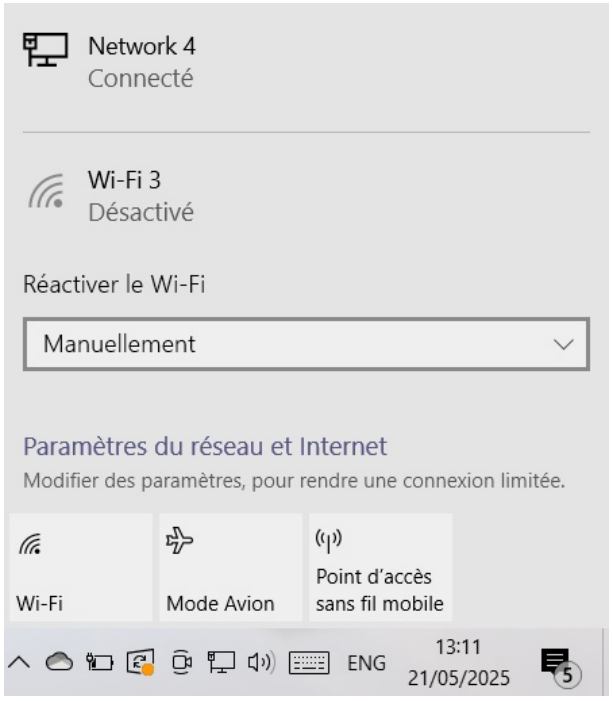

FIGURE 2.5 – Connexion réseau de Windows

2.4.3 Implémentation d'un serveur proxy

Au départ, nous avons mis en place un serveur proxy Squid pour assurer le partage de la connexion Internet. Il s'agit d'une solution open-source utilisée sous Linux, qui permet de gérer les connexions réseau et d'appliquer des règles spécifiques, telles que le blocage de certains sites web.

Cette configuration nous a permis de filtrer le trafic sortant selon des critères bien définis (adresses IP, noms de domaine, etc.), afin de restreindre l'accès à certains contenus sur le réseau.

Le schéma ci-dessous illustre clairement ce fonctionnement : l'utilisateur envoie une requête via le proxy, lequel vérifie si le site demandé est autorisé. Si ce dernier figure dans la liste des sites bloqués, le proxy refuse l'accès, et la demande n'atteint pas Internet.

FIGURE 2.6 – Schéma d'un accès restreint via un proxy

2.4.3.1 Installation du Squid (Serveur)

L'installation de **Squid Proxy** sur Kali Linux se fait en quelques étapes simples. Ce serveur proxy permet de filtrer, surveiller et mettre en cache le trafic web. Voici les étapes suivies :

— **Mettre à jour les paquets du système** :

Avant toute installation, il est recommandé de mettre à jour la base de données des paquets afin de s'assurer que les versions les plus récentes des logiciels seront utilisées. Cette opération s'effectue à l'aide de la commande suivante :

```
sudo apt update  sudo apt upgrade -y
```

— **Installer Squid** :

L'installation de Squid se fait via le gestionnaire de paquets APT :

```
sudo apt install squid -y
```

— **Vérification l'état du service Squid** :

Une fois l'installation terminée, il est possible de s'assurer que le service fonctionne correctement en vérifiant son état :

```
sudo systemctl status squid
```

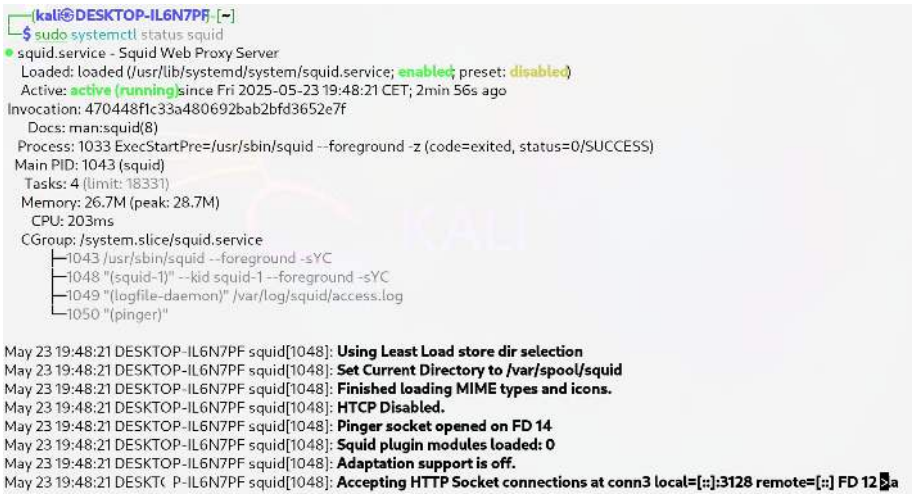

FIGURE 2.7 – Vérification de l'état du service Squid

— **Fichier de configuration principal** :

Le fichier de configuration principal de Squid est situé à l'emplacement suivant :

FIGURE 2.8 – Ouverture du fichier de configuration Squid

C'est dans ce fichier que l'on définit les règles de filtrage, les ports utilisés, les accès autorisés et l'ensemble des paramètres de fonctionnement du proxy. .

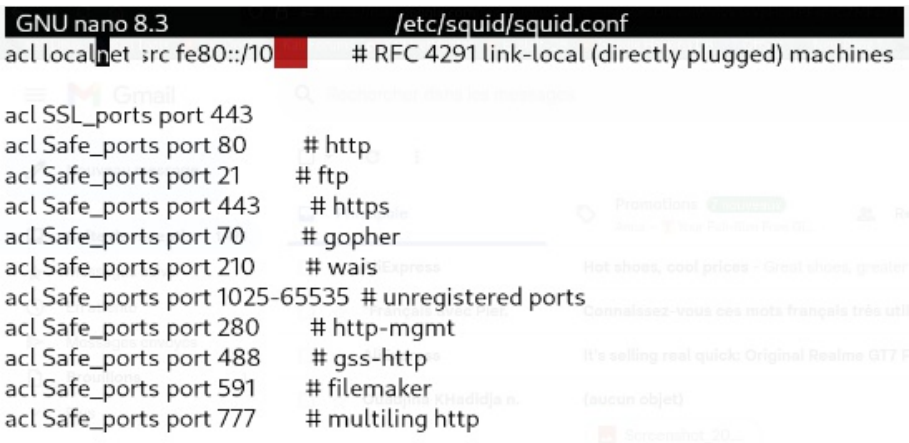

FIGURE 2.9 – Configuration Squid

La configuration du proxy a été effectuée au préalable sur le poste client, afin d'assurer une communication correcte avec le serveur, comme le montre la figure 2.9.

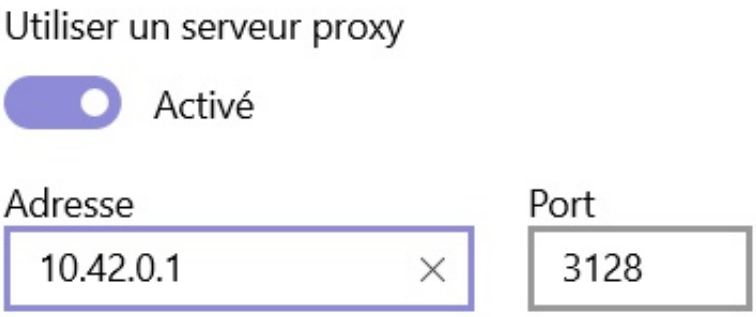

FIGURE 2.10 – Configuration du proxy côté client

L'interface de Squid affiche clairement que le poste client a été connecté avec succès au serveur.

2.4.3.2 Règles de blocage des sites web

Pour contrôler l'accès à certains sites web dans notre réseau, nous avons utilisé Squid, un proxy open source.

Voici comment nous avons procédé pour bloquer YouTube et Facebook. Nous avons ajouté deux ACL (Access Control Lists) qui permettent de repérer les sites à bloquer.

Ensuite, nous avons utilisé les règles http access deny pour interdire l'accès aux domaines définis.

```
http_access allow all
#blouquer youtube
acl block_youtube dstdomain .youtube.com .googlevideo.com
http_access deny block_youtube
#bloquer facebook
acl block_facebook dstdomain .facebook.com
http_access deny block_facebook
```

FIGURE 2.11 – Blocage des sites

2.5 Installation des logiciels de VPN client

Dans cet état, nous avons installé des logiciels VPN tels que l'HolaVPN, OpenVPN et le ProtonVPN.

Ces outils chiffrent notre trafic et le font transiter par des serveurs distants, ce qui dissimule notre localisation réelle et permet de contourner les restrictions imposées par certains réseaux ou gouvernements, rendant ainsi accessibles des sites normalement bloqués ou censurés.

2.5.1 Proton VPN

Proton VPN est un service de réseau privé virtuel (VPN) développé par la société suisse Proton Technologies AG, également éditrice du service de messagerie Proton Mail. Il offre une navigation sécurisée et privée en chiffrant le trafic internet des utilisateurs, permettant ainsi d'accéder à des contenus bloqués et de préserver l'anonymat en ligne. Le service utilise des protocoles sécurisés comme OpenVPN, IKEv2 et WireGuard avec un chiffrement AES-256, et applique une politique stricte de non-conservation des logs. [39]

La **figure 2.12** montre l'interface de création d'un compte ProtonVPN, où l'utilisateur saisit son e-mail, nom d'utilisateur et mot de passe avant de valider l'inscription.

FIGURE 2.12 – Création d'un compte

La **figure 2.13** présente l'interface de connexion de ProtonVPN, permettant à l'utilisateur de saisir ses identifiants pour accéder au service.

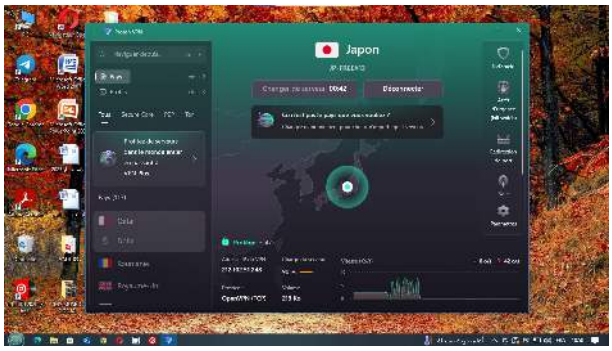

FIGURE 2.13 – Interface du logiciel ProtonVPN

2.5.2 OpenVPN

OpenVPN est un logiciel open-source qui permet la création de réseaux privés virtuels (VPN). Il utilise des protocoles de cryptage sécurisés, notamment SSL/TLS, pour per-

mettre la connexion sécurisée entre les utilisateurs et les serveurs, même sur des réseaux publics.

OpenVPN est largement utilisé pour fournir une solution VPN flexible et personnalisable, capable de contourner les restrictions géographiques et de garantir la confidentialité des utilisateurs. [40]

La **figure 2.14** présente l'interface d'OpenVPN dédiée à l'importation de profil, utilisée pour configurer une connexion VPN.

FIGURE 2.14 – Interface du logiciel OpenVPN

La **figure 2.15** illustre l'écran de connexion d'OpenVPN une fois le profil importé, permettant de renseigner les identifiants et d'établir la connexion sécurisée.

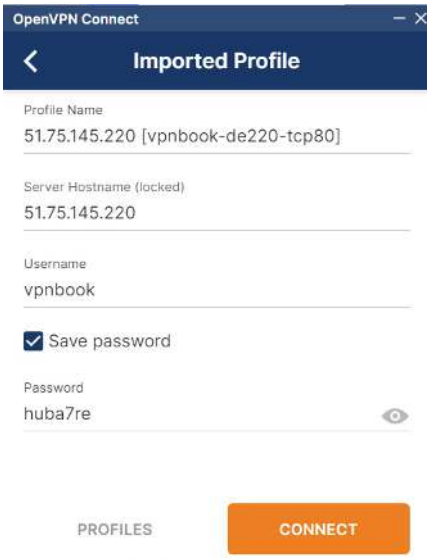

FIGURE 2.15 – Ajouter un VPN

La **figure 2.16** montre l'interface d'OpenVPN une fois la connexion établie, affichant le profil actif, l'état «Connected» ainsi que les statistiques de trafic en temps réel.

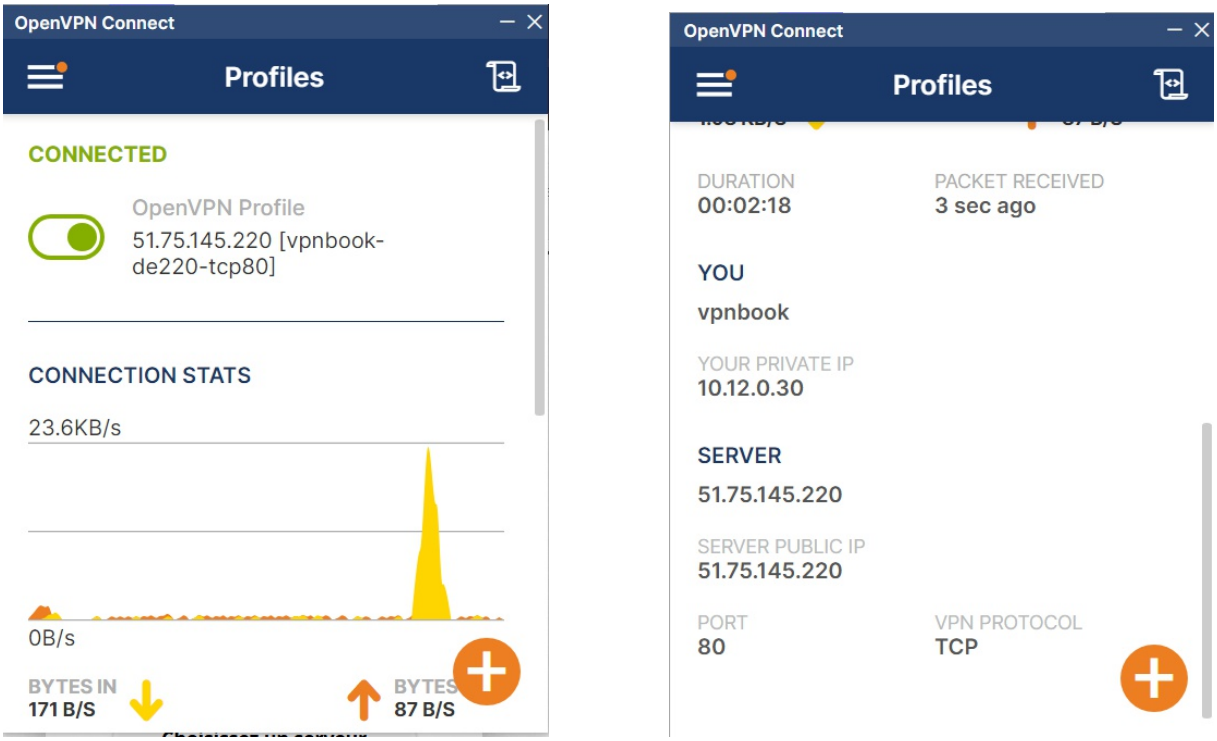

FIGURE 2.16 – Activation de VPN

2.5.3 HolaVPN

HolaVPN est un service de réseau privé virtuel (VPN) basé sur un modèle peer-to-peer (P2P). Contrairement aux VPN traditionnels, HolaVPN permet aux utilisateurs de partager leurs ressources de bande passante pour faciliter la navigation anonyme et sécurisée. Cependant, étant donné son modèle P2P, HolaVPN a suscité des préoccupations en matière de sécurité et de confidentialité des données, car il utilise la bande passante des utilisateurs pour acheminer le trafic d'autres personnes. [41]

La **figure 2.17** illustre l'écran de connexion à l'application Hola App via un compte Google, nécessitant la saisie du mot de passe pour accéder au service.

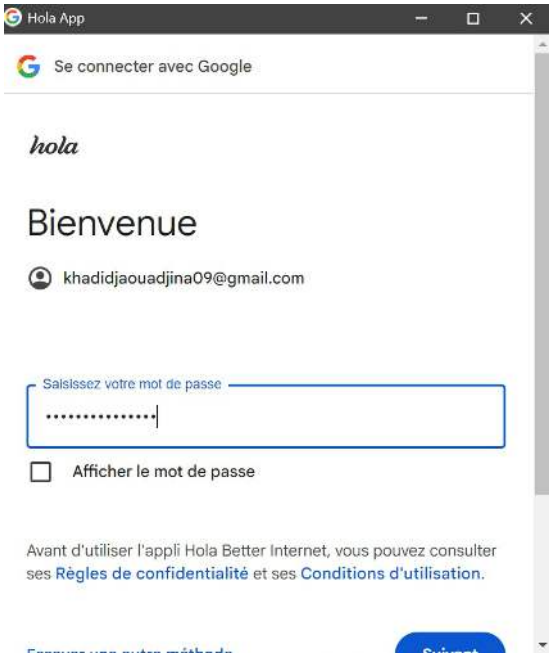

FIGURE 2.17 – Création d'un compte

La **figure 2.18** montre l'interface principale de l'application Hola App après connexion, indiquant le pays de navigation sélectionné (ici le Canada) ainsi qu'un bouton pour se déconnecter de la session VPN en cours.

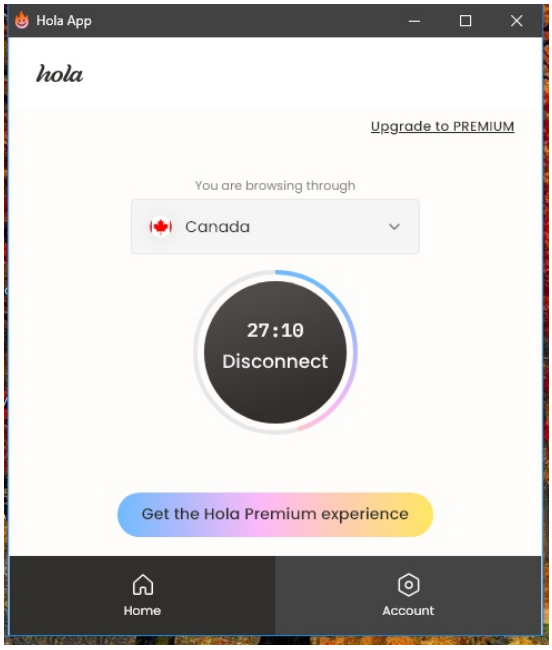

FIGURE 2.18 – Interface du logiciel HolaVPN

2.6 Installation des logiciels du surveillances côté serveur

À côté des outils open source de visualisation et de supervision, les solutions propriétaires sous licence, telles que PRTG ou OpManager, sont fréquemment privilégiées par les entreprises ayant des besoins de surveillance réseau plus avancés.

2.6.1 OpManager

2.6.1.1 Architecture de OpManager

La **figure 2.19** représente l'architecture de communication d'OpManager. Le logiciel centralise les données provenant des équipements réseau et les affiche via un tableau de bord. En cas d'incident, il peut envoyer des alertes par e-mail, SMS, application mobile ou support client, et déclencher des actions automatiques grâce à des workflows. Cela permet une surveillance efficace et proactive du réseau

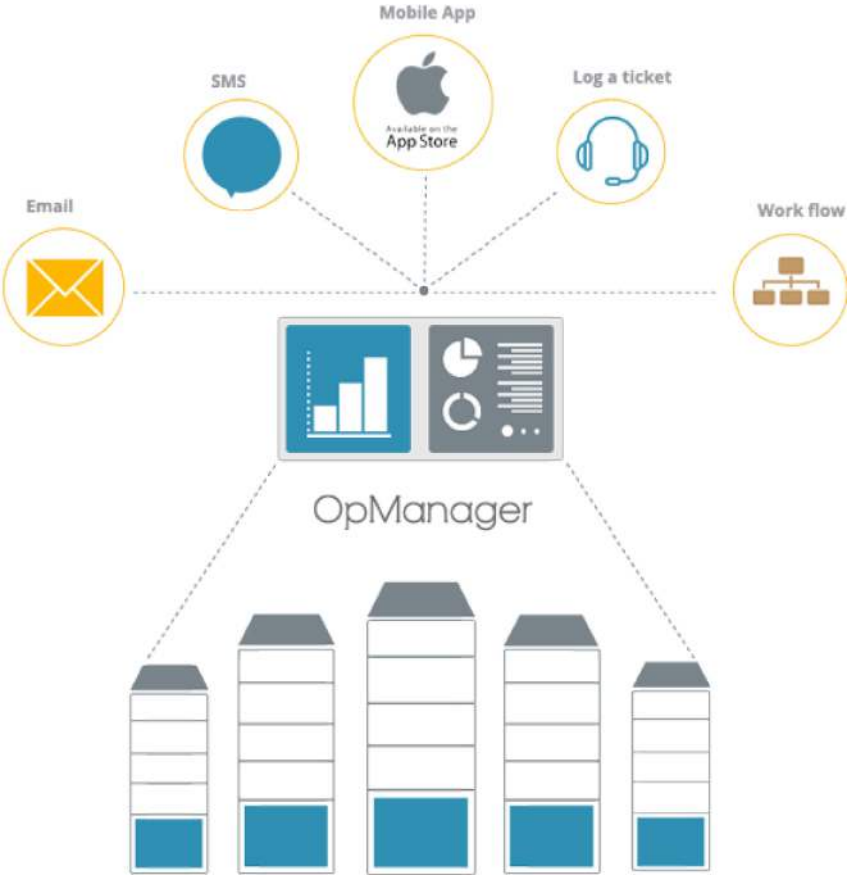

FIGURE 2.19 – Architecture de Opmanager [9]

2.6.1.2 installation de Opmanager

OpManager est un outil de supervision réseau complet. L'installation a été réalisée sous Kali Linux en suivant les étapes ci-dessous :

1. Télécharger le fichier d'installation depuis le site officiel de ManageEngine.
2. Rendre le fichier exécutable avec la commande :

   `chmod +x ManageEngine`$_{OpManager_*.bin}$

3. Lancer l'installation avec :

   `sudo ./ManageEngine`$_{OpManager_*.bin}$

4. Suivre les étapes de l'assistant d'installation.
5. Démarrer le service OpManager :

   ```
   cd /opt/ManageEngine/OpManager/bin sudo ./startOpManager.sh
   ```

```
┌──(kali㉿DESKTOP-IL6N7PF)-[/opt/ManageEngine/OpManager/bin]
└─$ sudo /opt/ManageEngine/OpManager/bin/run.sh

/opt/ManageEngine/OpManager/bin/..
/opt/ManageEngine/OpManager/bin/..
May 21, 2025 12:28:57 PM com.adventnet.persistence.ConfigurationParser$1 resolveEntity
INFO: Processing /opt/ManageEngine/OpManager/bin/../conf/product-config.xml
May 21, 2025 12:28:58 PM com.adventnet.persistence.ConfigurationParser$1 resolveEntity
INFO: Processing /opt/ManageEngine/OpManager/bin/../conf/customer-config.xml

----------------------------------------
Port      Availability      Module
----------------------------------------
8061          Yes          Client
13306          No          postgres
22            Yes          SSHD
69            Yes          TFTP
514           Yes          Syslog

############################################################
```

FIGURE 2.20 – Installation Opmanager

On suit les instructions. On accepte les conditions d'utilisation, on choisit où installer le logiciel

6. Accéder à l'interface web via le port 8061 :

```
http://[10.42.0.174:8060
```

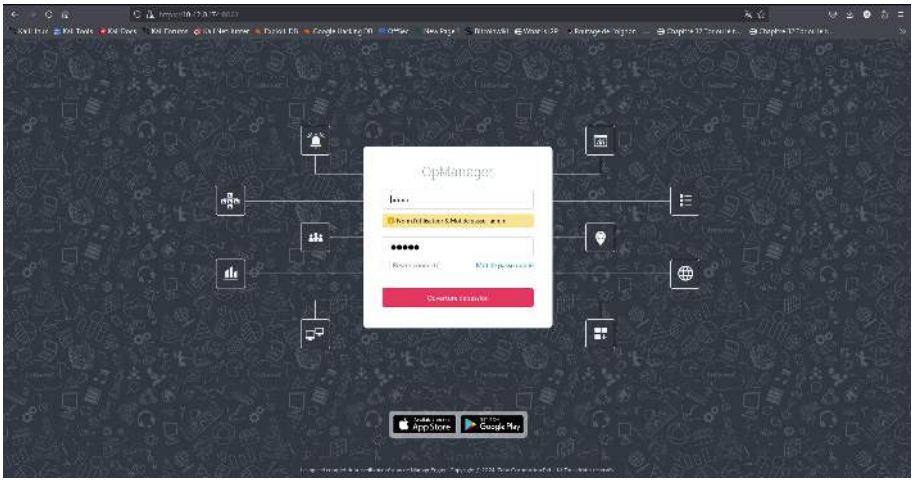

FIGURE 2.21 – Interface de connexion

Il faut patienter pendant le processus d'installation, qui peut durer quelques minutes. Une fois l'installation terminée, nous lançons OpManager et nous nous connectons à l'aide de notre compte utilisateur. enfin,On peut commencer à configurer et à surveiller notre réseau.

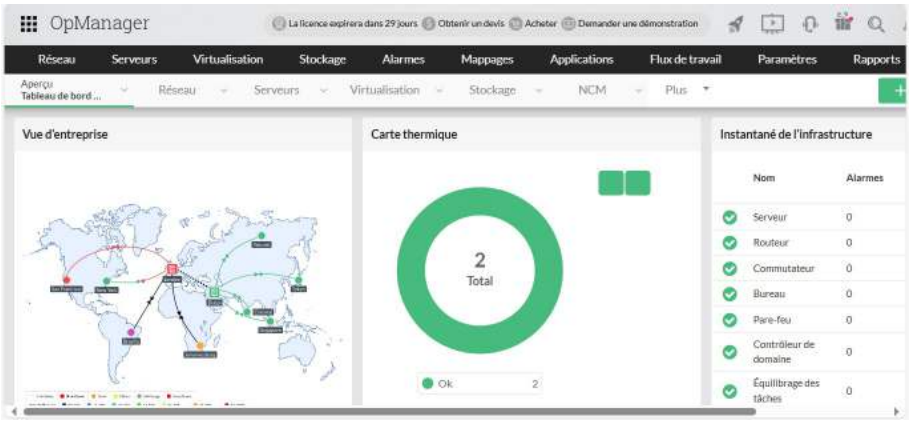

FIGURE 2.22 – Tableau de bord du logiciel OpManager

2.6.1.3 Fonctionnalites de Opmanager

OpManager propose une gamme complète de fonctionnalités destinées à assurer une supervision proactive et centralisée des infrastructures IT. Voici les principales fonctionnalités offertes par cet outil :

1. Surveillance réseau en temps réel : Contrôle continu de la santé, disponibilité et performances des équipements réseau (routeurs, commutateurs, pare-feu, points d'accès Wi-Fi, liaisons WAN, etc.) et des serveurs physiques et virtuels (Windows, Linux, VMware, Hyper-V, etc.).
2. Découverte automatique des appareils : Identification et cartographie automatique des équipements et ressources réseau, avec mappage hiérarchique et basé sur la localisation.
3. Gestion des performances : Suivi détaillé des indicateurs clés comme CPU, mémoire, bande passante, trafic réseau, et analyse des causes profondes des problèmes.
4. Alertes et notifications : Envoi d'alertes en temps réel par e-mail, SMS, appels ou pop-ups pour prévenir les équipes IT des incidents ou anomalies détectés, avec escalade automatique si nécessaire.
5. Analyse et rapports personnalisés : Tableaux de bord configurables, rapports détaillés sur la disponibilité, la performance, la bande passante, et analyses historiques pour faciliter la prise de décision.

2.6.2 PRTG

2.6.2.1 Architecture de PRTG

La **figure 2.23** montre l'architecture distribuée de PRTG, avec un serveur central et plusieurs sondes distantes déployées sur différents sites (locaux, distants, hébergés). Chaque sonde collecte localement les données de supervision et les transmet de façon sécurisée au serveur principal via Internet.

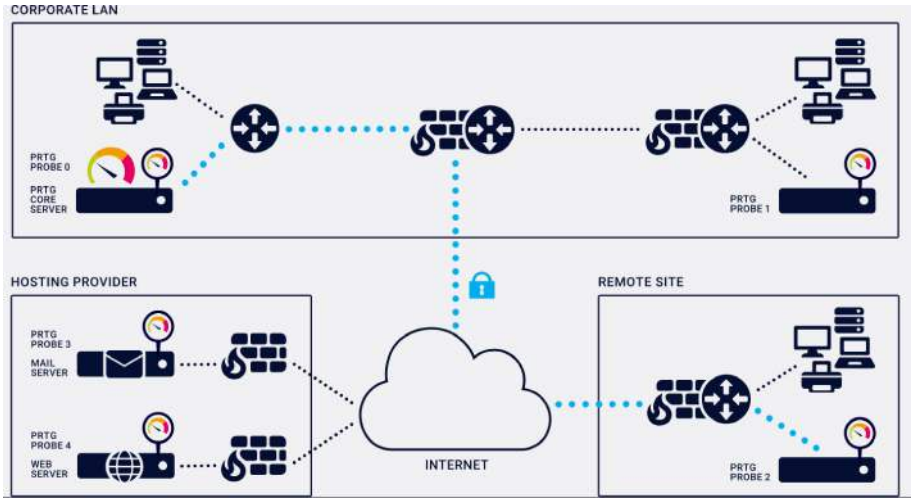

Figure 2.23 – Architecture de PRTG [10]

2.6.2.2 Installation de logiciel

Nous répétons les mêmes étapes que pour OpManager, nous téléchargeons PRTG depuis son site officiel en récupérant le fichier d'installation approprié.

— Démarrer le service Prtg :

```
start /wait PRTG Network Monitor Installer.exe
```

On lance l'installation. Ensuite, nous acceptons les conditions d'utilisation et sélectionnons une clé de licence. Après avoir lancé le logiciel, nous créons un compte en choisissant un nom d'utilisateur et un mot de passe. Une fois cette étape terminée, nous ouvrons PRTG, nous nous connectons, et nous sommes prêts à surveiller l'activité du réseau.

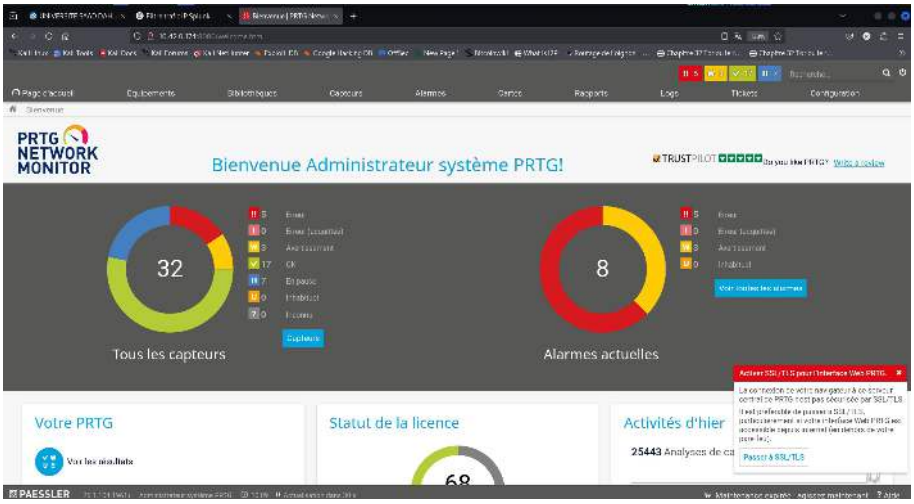

FIGURE 2.24 – Tableau de bord de PRTG

2.6.2.3 Fonctionnalites de PRTG

PRTG Network Monitor se caractérise par sa richesse fonctionnelle et sa flexibilité, offrant des outils performants pour assurer une supervision complète des infrastructures réseau. Voici ses principales fonctionnalités :

1. Supervision réseau complète : surveillance en temps réel de la bande passante, des serveurs, des équipements réseau, des applications, des environnements virtuels, etc.
2. Capteurs personnalisables :Environ 200 types de capteurs prédéfinis sont disponibles pour couvrir tous les aspects du réseau et des systèmes.
3. Tableaux de bord et visualisation : Création de cartes topologiques et tableaux de bord personnalisés en glisser-déposer avec plus de 300 widgets disponibles.
4. Technologies et protocoles supportés : Support de nombreux protocoles comme SNMP, WMI, SSH, HTTP.
5. Supervision distribuée :Surveillance multi-sites avec sondes distantes qui collectent les données localement et les transmettent au serveur central.

2.7 Conclusion

Dans ce chapitre, nous avons procédé à l'installation des différents logiciels nécessaires à la mise en œuvre de notre solution VPN, notamment le proxy Squid, les clients VPN, ainsi que les outils de surveillance réseau. Nous avons également détaillé la topologie du

réseau utilisée et expliqué l'architecture mise en place, incluant le rôle de chaque poste, les connexions physiques, et le cheminement du trafic Internet.

Dans le prochain chapitre, nous effectuerons différents tests pour observer le comportement du réseau. Nous analyserons notamment comment le VPN permet de contourner les restrictions du proxy, comment les outils de supervision réagissent à ces tentatives, et quelles données peuvent être collectées pour évaluer l'efficacité du dispositif mis en place. Ces tests nous permettront d'apprécier les forces et les limites de notre solution dans un contexte de supervision du trafic VPN.

Chapitre 3

Tests et supervision du VPN

3.1 Introduction

Après avoir validé le bon fonctionnement de notre architecture VPN supervisée, nous entamerons une série de tests pratiques visant à évaluer son efficacité. L'objectif est de vérifier si ces VPN permettent de contourner les restrictions et d'accéder aux sites bloqués. Une fois l'accès confirmé, nous superviserons les activités du client depuis le serveur à l'aide des outils de monitoring, afin d'analyser le comportement du réseau et détecter toute tentative de contournement ou de connexion suspecte.

3.2 Tests de connectivité

Avant l'installation du proxy ou du VPN, un test de connectivité a été effectué afin de vérifier que la machine cliente pouvait accéder librement à Internet, sans aucune restriction.

— Pour Serveur :

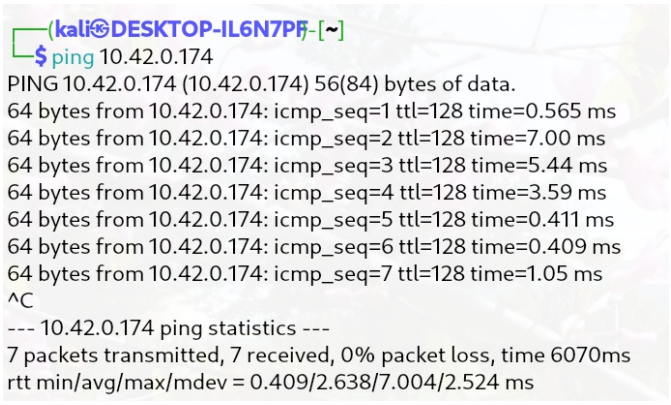

Figure 3.1 – Test ICMP Serveur

— Pour client :

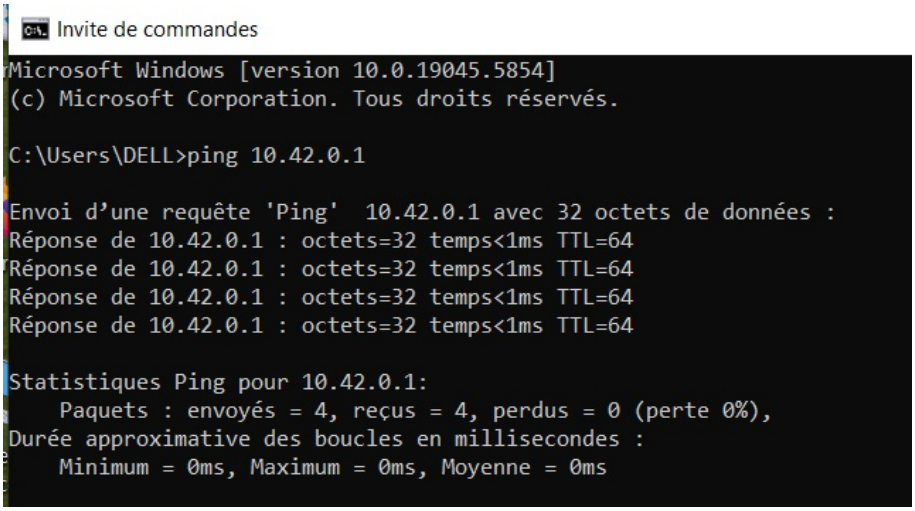

FIGURE 3.2 – Test ICMP Client

Les tests ICMP confirment une bonne connectivité entre le client et le serveur, sans perte de paquets et avec des temps de réponse faibles, ce qui indique un réseau stable et fonctionnel.

3.3 Déploiement et vérification du Proxy

Après avoir configuré les proxys et mis en place les règles de blocage des sites, nous procédons à une phase de test afin de vérifier si les sites ciblés sont effectivement bloqués ou toujours accessibles, comme illustré dans les figures 3.3 et 3.4.

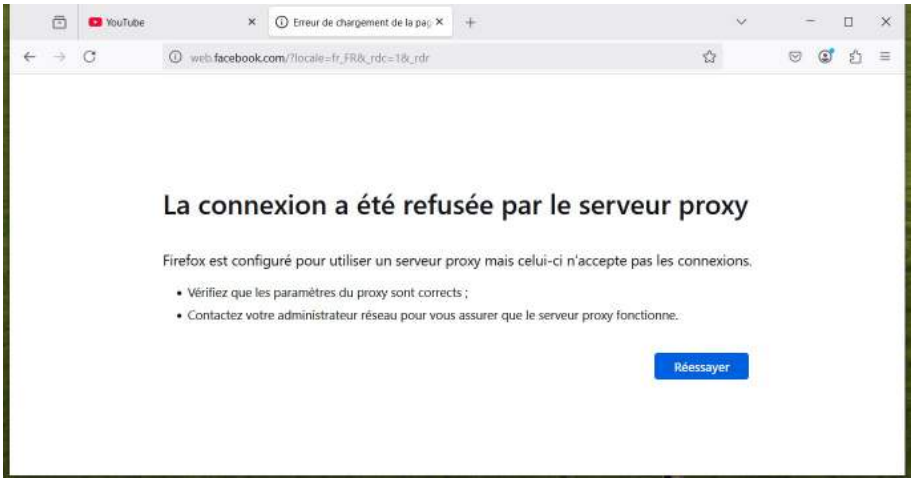

FIGURE 3.3 – Test de Proxy (Client)

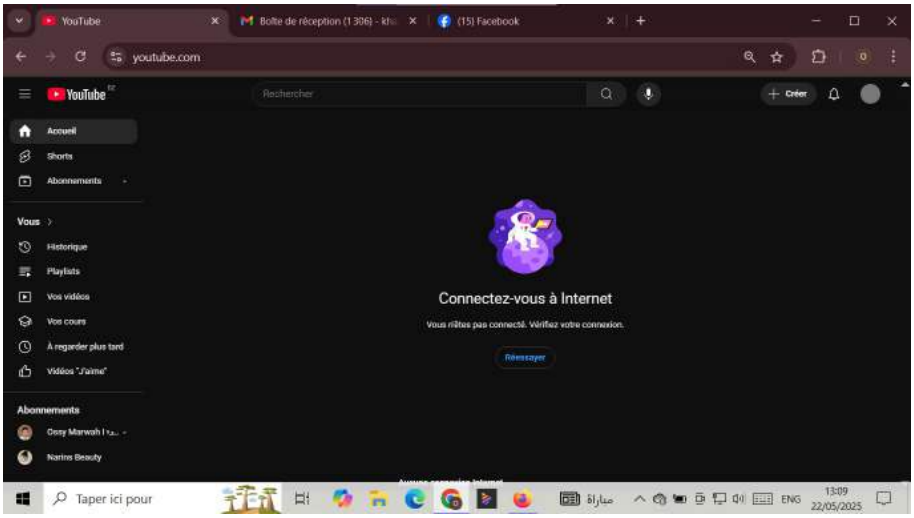

FIGURE 3.4 – Test 2 de Proxy (Client)

Les règles de filtrage bloquent l'accès aux sites ciblés, ce qui montre que le proxy fonctionne correctement.

3.4 Implémentation d'un VPN

Dans cette section, nous avons testé trois solutions VPN différentes : ProtonVPN, Hola VPN et OpenVPN.L'objectif était d'évaluer leur efficacité à contourner un proxy filtrant mis en place précédemment, ainsi que d'analyser leur comportement réseau en situation réelle.

Le schéma ci-dessous illustre le principe général de cette approche :lorsqu'un utilisateur tente d'accéder directement à un site bloqué, la requête est interceptée par le proxy d'entreprise, et l'accès est refusé. En revanche, en passant par un serveur VPN , la requête est chiffrée et redirigée, ce qui permet de contourner le filtrage du proxy et d'accéder au contenu bloqué.

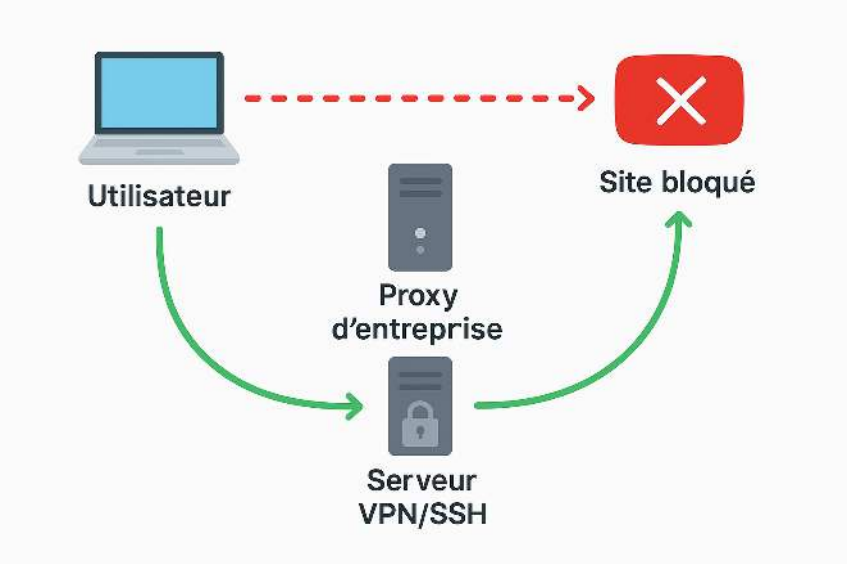

FIGURE 3.5 – Contournement d'un Proxy via un VPN

3.4.1 Test ProtonVPN

ProtonVPN est un service VPN suisse réputé pour sa sécurité, sa politique "no logs" et sa facilité d'utilisation.

3.4.1.1 Réalisation du test

La **figure 3.6** affiche un avertissement de ProtonVPN indiquant qu'un proxy est détecté, ce qui peut nuire à l'efficacité du VPN.

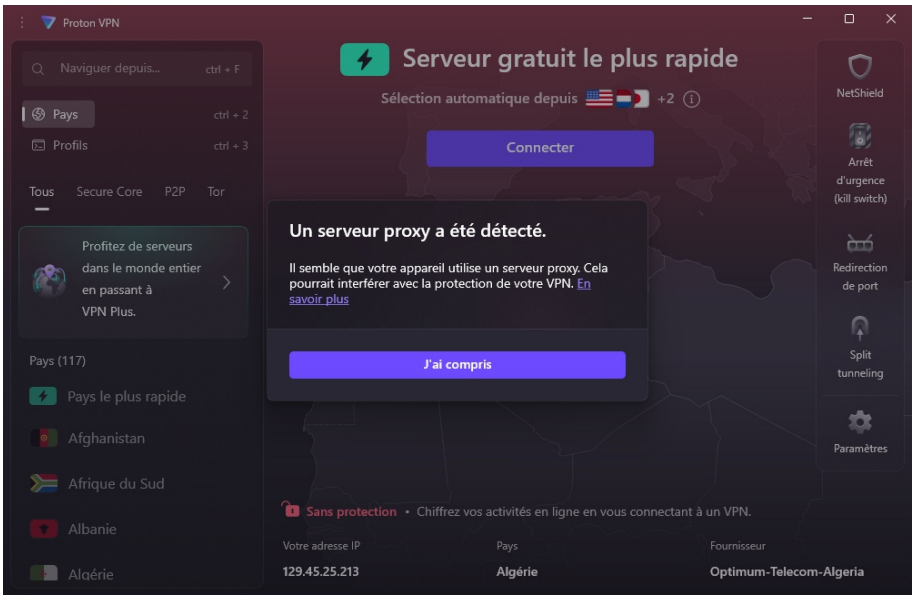

FIGURE 3.6 – Test proton

3.4.1.2 Résultat de test

— La connexion échoue lorsque le proxy est activé.
— Il tente de se connecter via des ports classiques bloqués (UDP 1194, TCP 443).
— ProtonVPN ne contourne le proxy qu'avec une configuration avancée ou un abonnement payant.

3.4.2 Test OpenVPN

OpenVPN est un logiciel libre très utilisé dans les environnements professionnels. Il permet une configuration fine et l'usage de divers ports et protocoles (UDP, TCP).

3.4.2.1 Réalisation du test

La **figure 3.7** illustre qu'une connexion VPN est établie via OpenVPN, permettant l'accès à Facebook malgré les éventuelles restrictions locales appliquées au réseau. L'interface confirme que le tunnel VPN est actif et transmet du trafic en temps réel.

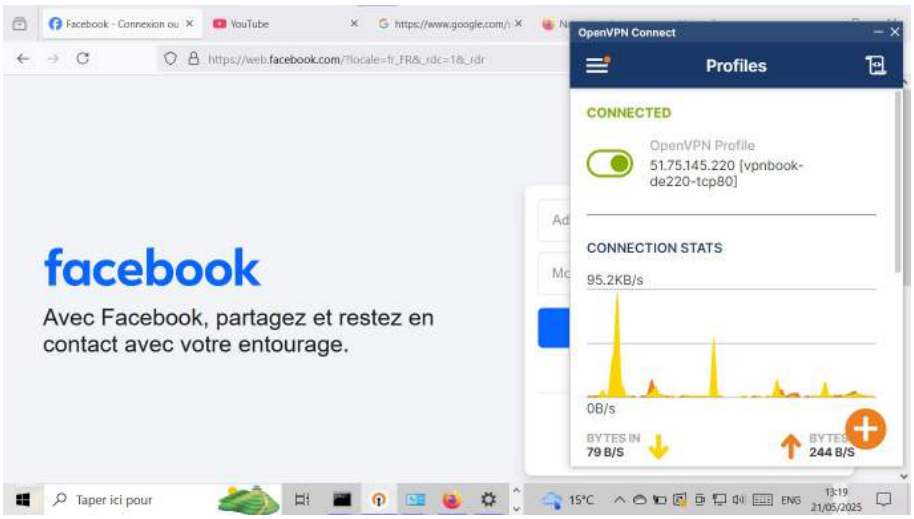

FIGURE 3.7 – Test OpenVPN

3.4.2.2 Résultat de test

— OpenVPN réussit à établir la connexion en utilisant le port TCP 443.
— OpenVPN contourne le proxy en ajustant le port et le protocole.
— Le tunnel VPN est bien établi et chiffré.

3.4.3 Test HolaVPN

Hola VPN est un VPN de type "peer-to-peer" qui fonctionne via une extension de navigateur. Il redirige le trafic en passant par d'autres utilisateurs connectés au réseau Hola.

3.4.3.1 Réalisation du test

La **figure 3.8** montre que l'application Hola VPN est connectée via un serveur localisé au Canada, permettant l'accès à YouTube en contournant les restrictions géographiques.

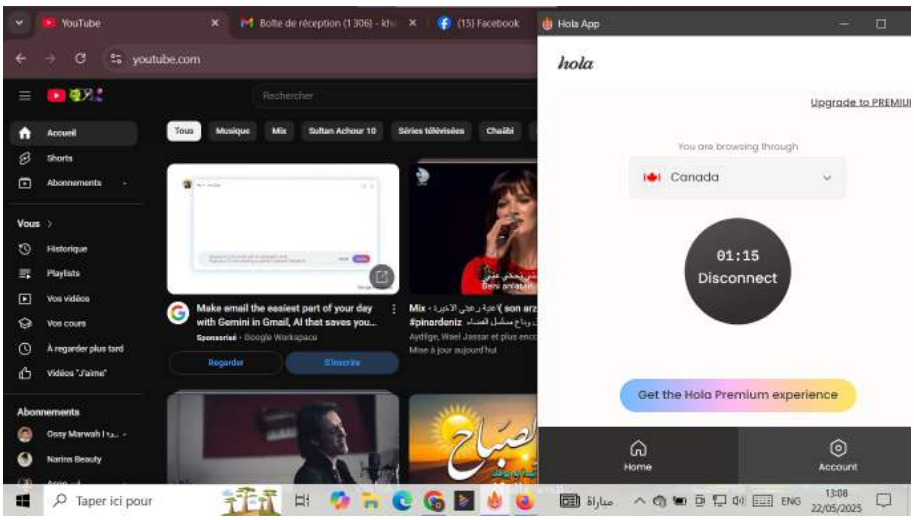

FIGURE 3.8 – Test HolaVPN

3.4.3.2 Résultat du test

— Le site reste accessible via l'extension Hola, même lorsque le proxy est activé.
— Hola VPN contourne le proxy facilement, mais son modèle P2P expose à des risques de sécurité.

3.4.4 Comparaison des solutions VPN

Parmi les trois solutions testées, Hola VPN et OpenVPN permettent de contourner efficacement les restrictions imposées par le proxy filtrant. Cependant, en matière de sécurité et de fiabilité, OpenVPN se distingue comme la solution la plus robuste et adaptée à un usage professionnel. Bien que très accessible, Hola VPN soulève d'importantes préoccupations en matière de confidentialité, en raison de son architecture pair-à-pair, et ne convient donc pas à des environnements nécessitant un haut niveau de sécurité.

Le tableau ci-dessous présente une comparaison synthétique des trois solutions selon plusieurs critères clés :Protocole utilisé, Port utilisé, sécurité, contourenement.

Critère	ProtonVPN	Hola VPN	OpenVPN
Protocole utilisé	OpenVPN, WireGuard	HTTP	OpenVPN (UDP/TCP)
Port utilisé	1194 UDP / 443 TCP	80 / 443 (navigateur)	TCP 80/443, UDP 53/25000
Interface	Application	Extension navigateur	Fichier config (.ovpn)
Sécurité	Élevée	Faible	Élevée
Facilité d'utilisation	Simple	Très simple	Moyennement simple
Contournement du proxy	Échec	Réussi	Réussi

Tableau 3.1 – Comparaison des solutions VPN testées

3.5 Surveillance et analyse du trafic

Une fois l'accès au site bloqué établi via le VPN, nous pouvons entamer la phase de supervision du trafic VPN.

Avant d'entamer toute supervision, il est essentiel de vérifier que le VPN est bien activé, puis de confirmer l'adresse IP attribuée en utilisant la commande ipconfig.

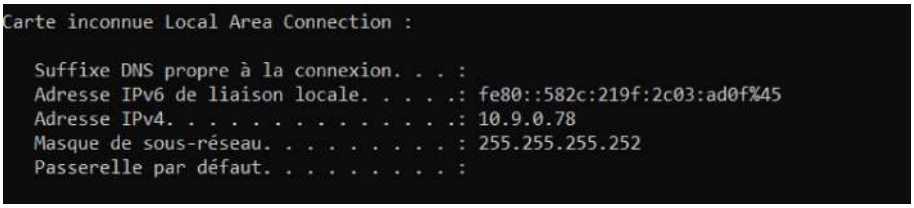

Figure 3.9 – Vérification de l'activation du OpenVPN

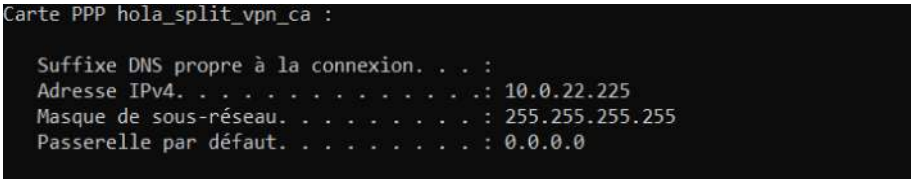

Figure 3.10 – Vérification de l'activation du HolaVPN

3.5.1 Surveillance du VPN avec OpManager

OpManager permet de surveiller en temps réel les connexions VPN, en suivant la disponibilité des tunnels, la latence et les pertes de paquets. Ses alertes et tableaux de bord facilitent la détection rapide des problèmes pour garantir une connexion stable aux utilisateurs distants.

La figure 3.11 illustre l'état d'un périphérique sous Windows 10, associé à l'adresse IP privée 10.9.0.38. Étant issue d'une plage d'adresses internes, cette IP est vraisemblablement attribuée par un VPN, suggérant que le périphérique est connecté à distance au réseau supervisé.

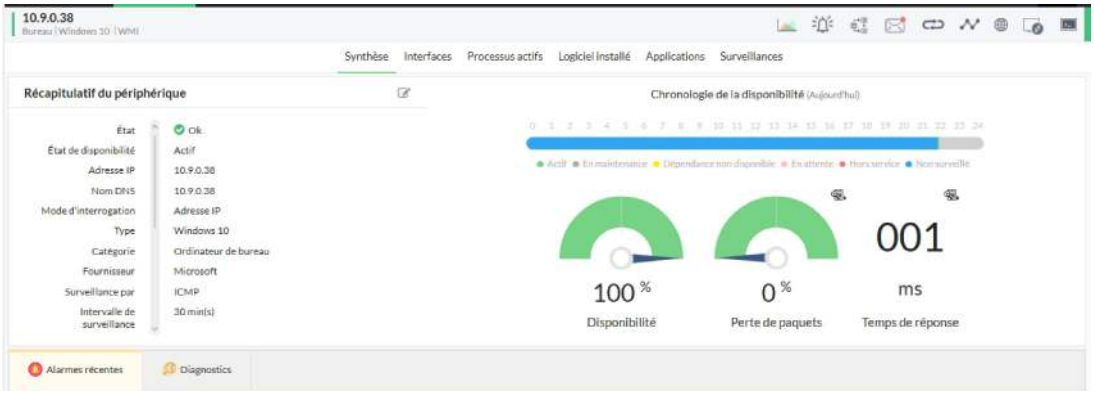

Figure 3.11 – État de disponibilité du poste

— OpenVPN est initialement mis en place comme serveur pour assurer des connexions sécurisées, puis OpManager prend le relais pour en surveiller en temps réel la disponibilité et les performances.

La **figure 3.12** présente un aperçu des performances du serveur Tomcat, avec une bonne réactivité et un suivi en temps réel de l'état et des ressources.

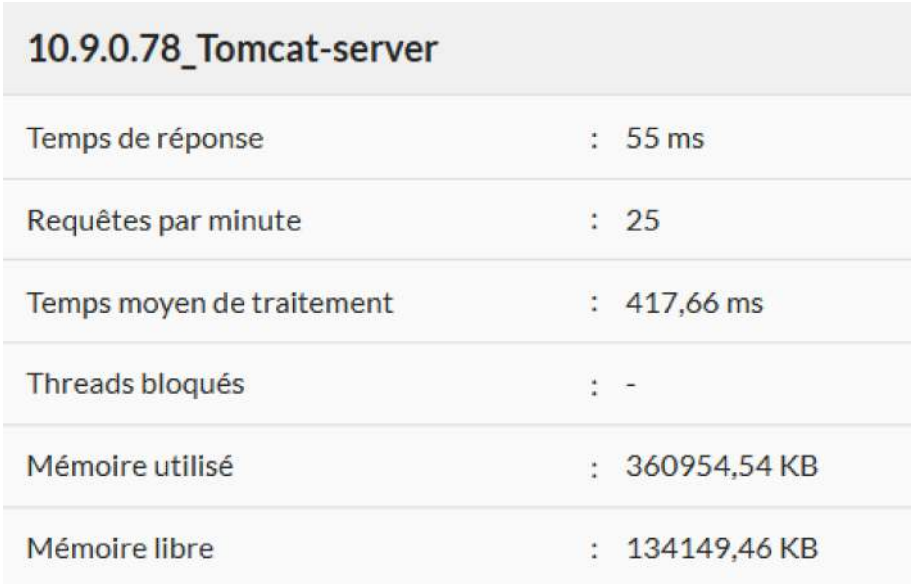

FIGURE 3.12 – Métriques de performance

La **figure 3.13** montre qu'un test de ping vers l'adresse 10.9.0.78 a réussi. Le paquet envoyé a bien reçu une réponse, sans aucune perte, et le temps de réponse est très rapide.

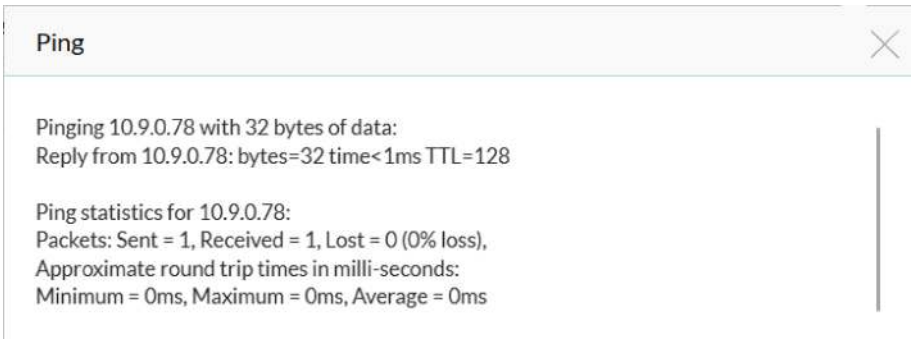

FIGURE 3.13 – Test Ping

La **figure 3.14** montre que le processus OpenVPN est actif, confirmant le bon fonctionnement du service VPN sur la machine.

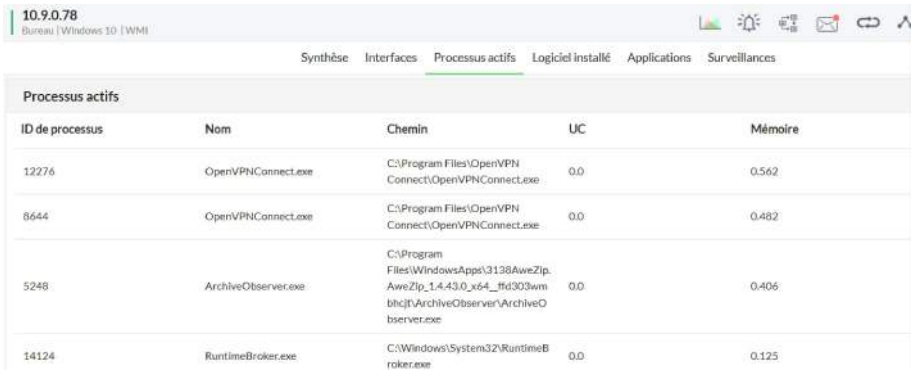

FIGURE 3.14 – Liste des processus actifs

La **figure 3.15** indique que la machine 10.9.0.78 est accessible sans latence notable, avec un seul saut détecté, ce qui confirme une connexion réseau directe et stable.

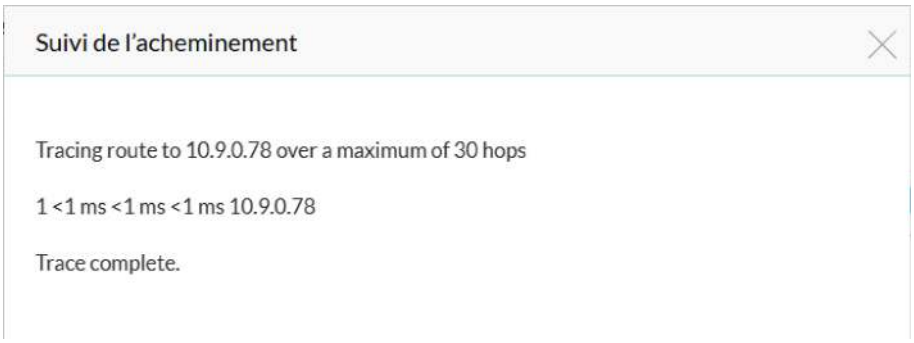

FIGURE 3.15 – Connectivité réseau

La **figure 3.16** confirme que le serveur Tomcat est en parfaite santé.

FIGURE 3.16 – État instantané du serveur

Ce schéma illustre la supervision centralisée des services par Applications Manager, qui contrôle plusieurs composants, dont Tomcat, PostgreSQL, et diverses applications distantes.

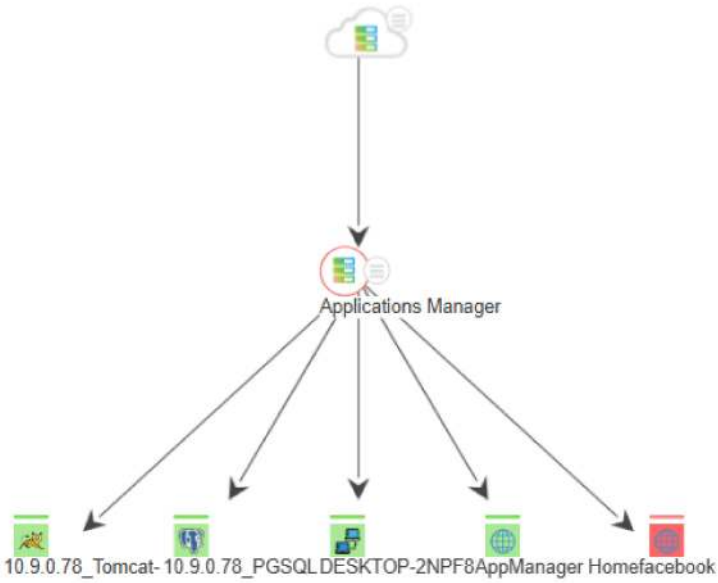

FIGURE 3.17 – Supervision centralisée des services

La **figure 3.18** montre une série d'alertes en temps réel générées par OpManager, indiquant des interruptions et rétablissements successifs de la connectivité réseau pour l'adresse IP 10.9.0.38. On y observe également un échec d'authentification WMI, suggérant des problèmes potentiels de stabilité ou de configuration réseau sur l'équipement surveillé.

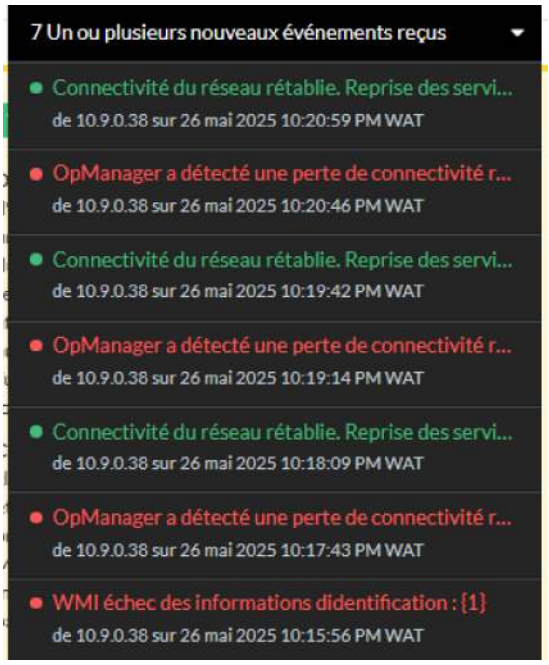

FIGURE 3.18 – Alertes en temps réel

La **figure 3.19** montre que le périphérique est en état critique , ce qui peut indiquer un problème logiciel ou une erreur de supervision.

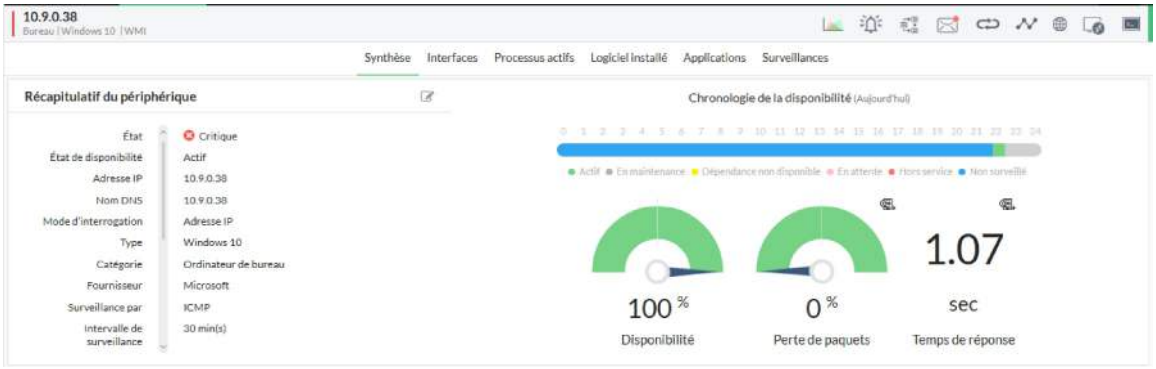

FIGURE 3.19 – État critique

La **figure 3.20** montre un graphique circulaire représentant les alarmes récentes détectées sur le réseau.

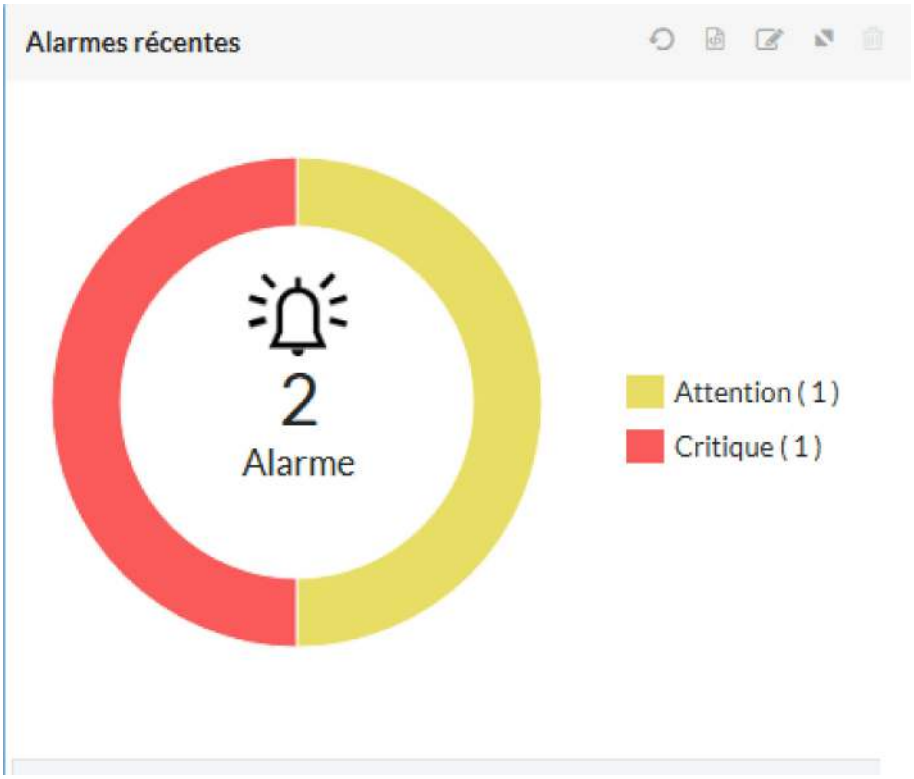

FIGURE 3.20 – Répartition des alarmes récentes détectées

— La couleur rouge indique un état critique, signifiant que le périphérique est éteint ou ne fonctionne pas correctement.
— La couleur jaune indique un état d'alerte nécessitant une attention particulière,

souvent lié à un composant physique du périphérique comme le processeur (CPU) ou la mémoire (RAM).

Après la désactivation d'OpenVPN, le ping vers l'adresse 10.9.0.78 échoue, indiquant une perte totale de connectivité, comme le montre la **figure 3.20**.

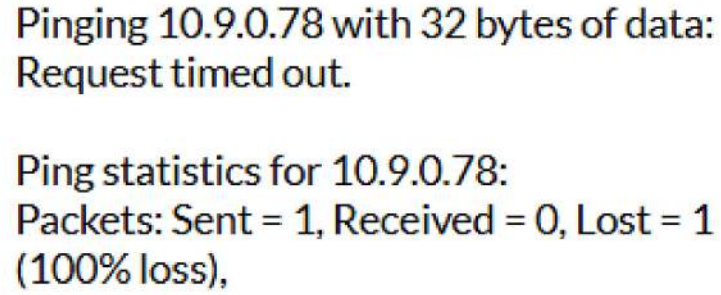

FIGURE 3.21 – Ping après désactivation

La **figure 3.22** illustre l'état de disponibilité du serveur, mettant en évidence un déséquilibre entre le temps de fonctionnement et les périodes d'indisponibilité. Elle permet d'évaluer rapidement la fiabilité du service sur la période observée.

FIGURE 3.22 – État global du serveur

Indicateur	Valeur
Temps total d'indisponibilité	47 Min. 49 Sec.
Pourcentage immobilisation totale	44.116%
Pourcentage du temps total de disponibilité	55.884%
Temps moyen de réparation (MTTR)	47 Min. 49 Sec.
Moyenne des temps de bon fonctionnement (MTBF)	1 H. 0 Min. 35 Sec.

Tableau 3.2 – Sommaire du temps d'indisponibilité/de disponibilité du moniteur

3.5.2 Surveillance du VPN avec PRTG

PRTG surveille en temps réel les connexions VPN en mesurant la disponibilité, la latence et les pertes de paquets. Ses capteurs et alertes automatiques permettent de détecter rapidement les anomalies pour garantir une connexion stable aux utilisateurs.

La **figure 3.23** présente l'interface de supervision du client VPN, montrant que le périphérique avec l'adresse IP 10.42.0.174 fonctionne correctement.

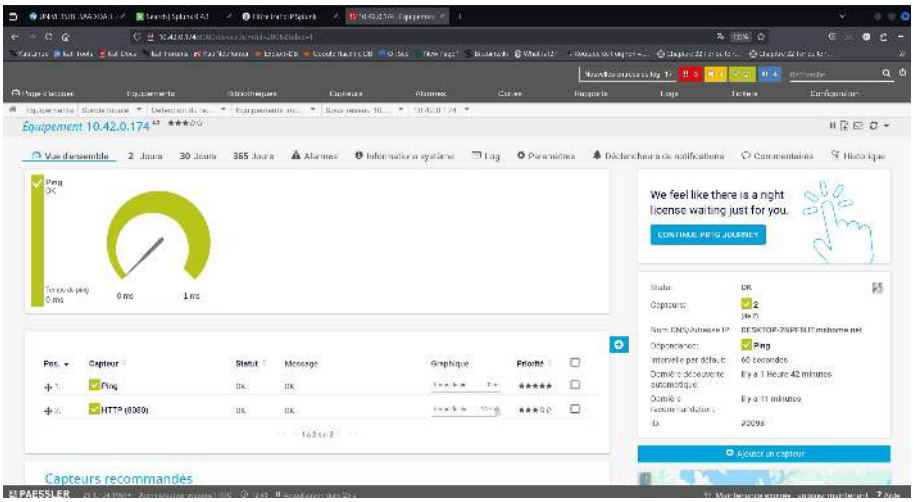

Figure 3.23 – État de supervision réseau du client

Cette supervision permet de s'assurer que le client VPN est accessible et que les services tels que HTTP sont opérationnels.

La **figure 3.24** montre les informations détaillées sur l'état d'un équipement réseau nommé DESKTOP-2NPF8UT.

FIGURE 3.24 – Détail de l'état d'un équipement

La **figure 3.25** illustre l'interface de supervision de l'équipement identifié par l'adresse IP 10.0.22.225, connecté via Hola VPN. Elle indique que le périphérique fonctionne correctement, avec un capteur en état normal et un autre en alerte mineure, permettant un suivi en temps réel de la performance et de la disponibilité du client VPN.

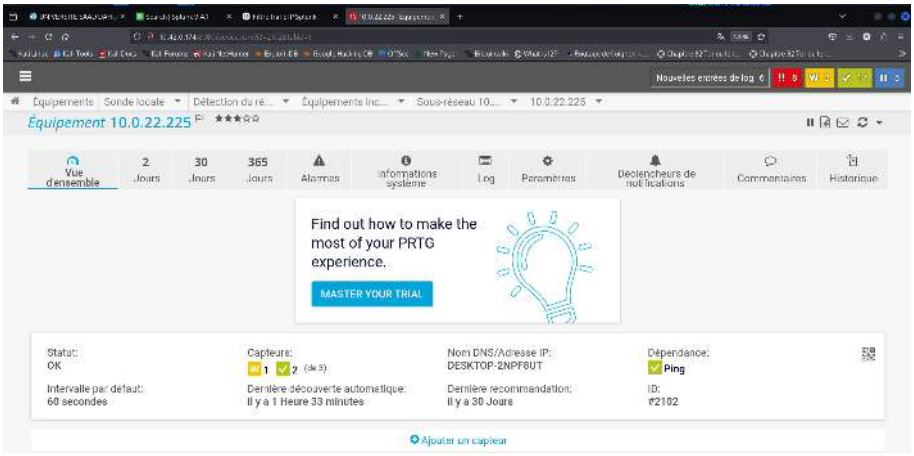

FIGURE 3.25 – Supervision du client VPN

La **figure 3.26** illustre l'interface de supervision PRTG pour l'équipement DNS avec l'adresse IP 8.8.8.8.

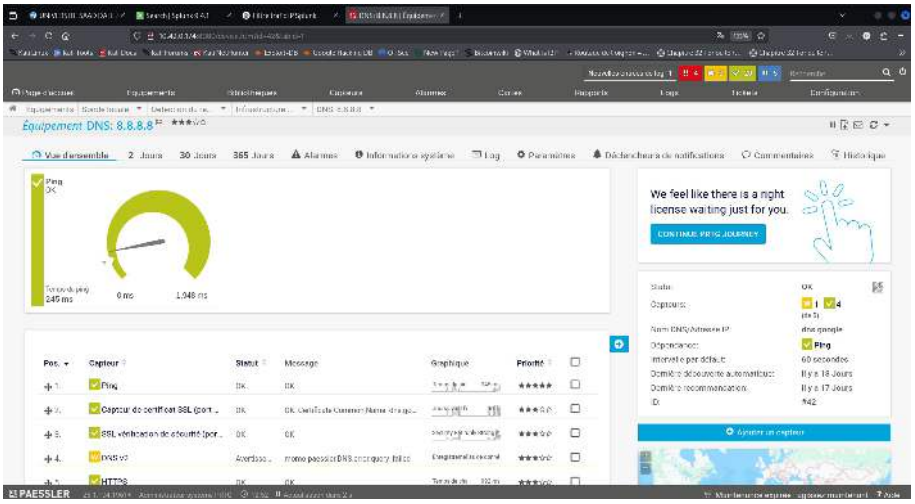

FIGURE 3.26 – Supervision DNS

Un code couleur est associé aux messages des capteurs, affiché en haut à droite du tableau de bord, comme illustré dans la figure 3.26.

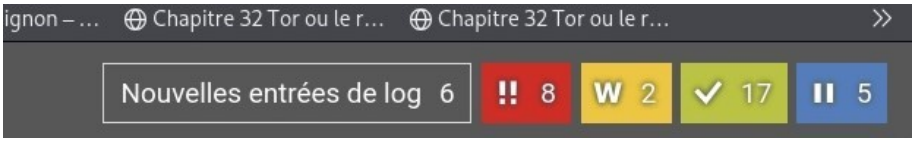

FIGURE 3.27 – Alertes du PRTG

— La couleur grise signifie qu'un événement s'est produit et a été enregistré dans le journal.
— La couleur rouge signale une erreur ou un échec de la collecte d'informations par un capteur.
— La couleur bleue désigne les capteurs qui ont été mis en pause.
— La couleur verte indique un fonctionnement normal des capteurs.

La **figure 3.28** illustre la vue globale de la supervision du réseau à travers PRTG Network Monitor, avec une organisation des équipements par catégories et par sous-réseaux détectés.

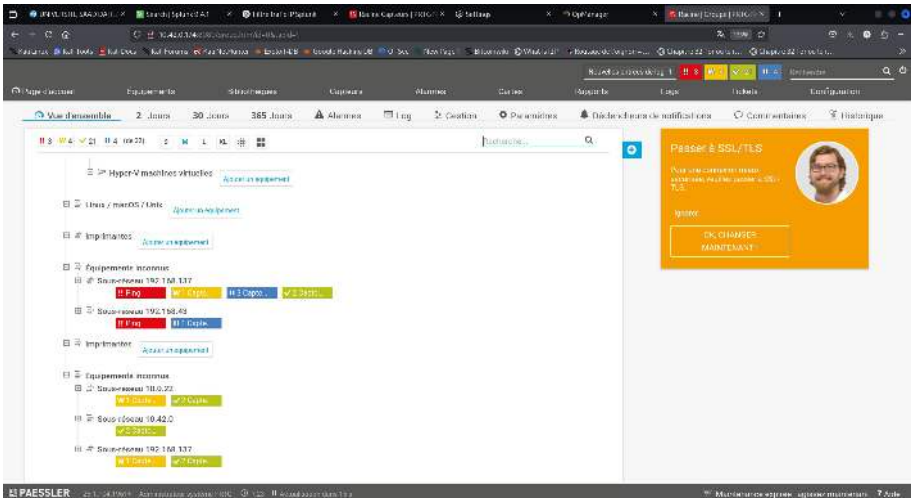

FIGURE 3.28 – Suivi temporel du trafic

La **figure 3.29** représente trois graphiques de surveillance générés par l'outil PRTG, chacun couvrant une période différente : à court terme (2 jours), moyen terme (30 jours) et long terme (365 jours).

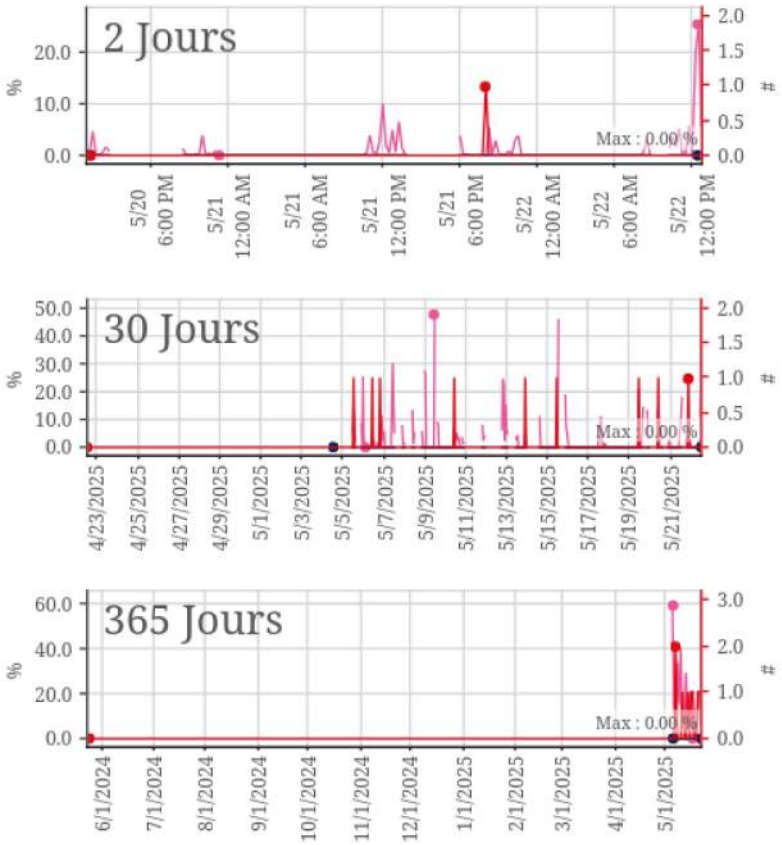

FIGURE 3.29 – les graphes de surveillance réseau

Ces graphiques permettent de visualiser l'évolution de plusieurs indicateurs clés tels que le trafic réseau, la charge CPU, le temps de réponse, ainsi que les alarmes déclenchées lors de dépassements de seuils critiques.

Chaque indicateur est représenté par une couleur spécifique, facilitant l'interprétation des données. Le tableau ci-dessous présente la correspondance entre ces couleurs et les éléments surveillés.

Couleur (symbole)	Élément surveillé	Signification / Utilité
Rouge	Alarmes	Indique qu'un seuil critique a été franchi. Représenté par des points rouges au sommet des pics.
Bleu foncé	Indice de temps de réponse	Représente les délais de réponse des services ou capteurs surveillés.
Vert cyan / Bleu clair	Indice de charge CPU	Reflète l'utilisation du processeur. Faible dans les données observées.
Rose clair	Taux de trafic	Indique le trafic réseau (entrant/sortant). Activité accrue sur certaines périodes.

Tableau 3.3 – Code couleur des indicateurs de surveillance réseau

3.5.3 OpManager vs PRTG

Parmi les solutions de supervision réseau, OpManager de ManageEngine et PRTG Network Monitor de Paessler se démarquent. OpManager, robuste et modulaire, est idéal pour les grandes infrastructures grâce à ses fonctionnalités avancées et son intégration avec la suite ManageEngine, bien qu'il demande une certaine expertise technique. À l'inverse, PRTG séduit par sa simplicité, son interface intuitive et son modèle basé sur les capteurs, le rendant parfait pour les PME. Il reste performant pour des environnements complexes, mais atteint ses limites dans les très grandes architectures.

3.6 Conclusion

Ce chapitre a permis de valider la solution VPN mise en place à travers la simulation de divers scénarios d'utilisation. Les tests de connectivité ont confirmé la stabilité du réseau, tandis que l'intégration du proxy s'est révélée efficace pour restreindre l'accès à certains contenus. L'évaluation des trois solutions VPN – ProtonVPN, OpenVPN et HolaVPN – a permis de mesurer leur capacité à contourner ces restrictions, mettant en évidence la fiabilité d'OpenVPN pour un usage professionnel sécurisé. Par ailleurs, la supervision du réseau à l'aide d'OpManager et de PRTG a démontré la complémentarité de ces deux

outils, en fournissant une analyse détaillée du trafic et une détection rapide des anomalies. L'ensemble de ces expérimentations souligne l'importance cruciale d'une supervision continue pour garantir la sécurité, la stabilité et les performances des infrastructures VPN au sein des environnements professionnels.

Conclusion Générale

Dans ce projet, nous avons conçu, déployé et évalué une solution de surveillance des réseaux VPN, répondant aux exigences croissantes en matière de cybersécurité, de performance réseau et de contrôle des accès en environnement professionnel.

La solution repose sur l'intégration de VPN sécurisés (OpenVPN, ProtonVPN, HolaVPN), d'un serveur proxy (Squid), ainsi que des outils de supervision réseau (OpManager et PRTG). Une architecture client-serveur simulée a été mise en place, incluant des configurations IP adaptées, un filtrage proxy pour le contrôle des accès, et une surveillance active des connexions en temps réel.

Le proxy Squid a été configuré afin de restreindre l'accès à certains sites web jugés non essentiels ou potentiellement distrayants, notamment les réseaux sociaux, les plateformes de streaming, ou encore certains services de messagerie en ligne. Cette restriction repose sur l'utilisation de listes de contrôle d'accès (ACL), associées à des règles spécifiques permettant de bloquer les connexions selon les URL, les adresses IP ou les types de contenu.

Dans un second temps, plusieurs services VPN tels que OpenVPN, ProtonVPN et Hola VPN ont été mis en œuvre dans le but de tester leur capacité à contourner les restrictions imposées par le proxy. Ces tests ont permis d'observer comment chaque solution VPN agit pour masquer le trafic utilisateur et bypasser les filtres de sécurité, en exploitant notamment des tunnels chiffrés ou des ports standards difficilement bloquables (comme le port 443 utilisé pour HTTPS).

Les outils de supervision réseau, OpManager et PRTG Network Monitor, ont été utilisés pour suivre en temps réel les comportements réseau. Grâce à ces outils, il a été possible de détecter les tentatives de contournement, identifier les flux anormaux, générer des alertes en cas de dépassement de seuils critiques, et surveiller la disponibilité ainsi que la performance des connexions VPN.

Ce travail nous a permis de renforcer nos compétences sur les architectures réseau, les protocoles de sécurité (SSL/TLS, IPsec), et les outils de supervision avancés. Il a également impliqué l'usage de systèmes Windows et Linux, ainsi qu'une interprétation

rigoureuse des données en conditions réalistes.

Cependant, plusieurs défis ont été rencontrés : l'intégration d'outils hétérogènes a exigé une coordination technique soignée, la gestion du trafic chiffré a parfois complexifié l'analyse, et la simulation d'activités suspectes de façon réaliste s'est révélée délicate.

Malgré ces obstacles, les tests ont confirmé la pertinence de la solution proposée. Les outils de supervision ont démontré leur efficacité en matière de détection d'intrusions, d'analyse du trafic et de gestion proactive des incidents.

Bibliographie

[1] (2023) Surfshark vpn. [Online]. Available : https://surfshark.com

[2] R. Tinhinan and S. Fadhila, *Étude et mise en place d'un réseau VPN*, 2017, mémoire de Master, Département Électronique, Faculté du Génie Électrique et Informatique.

[3] Mémoire online. [Online]. Available : https://www.memoireonline.com/

[4] SaaSkart, "Manageengine opmanager," https://www.saaskart.co/product/manageengine-opmanager, 2024.

[5] AlertOps, "Prtg integration guide," https://alertops.com/integrations/prtg/, 2024.

[6] J. Michaud, "Configurer les notifications par courriels avec nagios et gmail," https://www.jmichaud.ca/article/configurer-notifications-courriels-nagios-gmail/, 2023.

[7] T. Ministry, "Using zabbix and ntfy to monitor production software status for free," https://techministry.blog/2024/07/17/using-zabbix-and-ntfy-to-monitor-production-software-status-for-free/, 2024.

[8] TryHackMe, "Wazuh : Security information and event management," https://tryhackme.com/room/wazuhct, 2025.

[9] ManageEngine. (2025) Logiciel de surveillance réseau - manageengine opmanager. Consulté le 24 mai 2025. [Online]. Available : https://www.manageengine.com/fr/network-monitoring/

[10] Paessler AG. (2025) La surveillance centralisée dans les systèmes distribués. Consulté le 24 mai 2025. [Online]. Available : https://www.paessler.com/fr/learn/whitepapers/white_paper_managing_central_monitoring

[11] Y. Jin, M. Tomoishi, and S. Matsuura, "Enhancement of vpn authentication using gps information with geo-privacy protection," 2016 25th International Conference on Computer Communication and Networks (ICCCN), pp. 1–6, Aug. 2016.

[12] S. Eltanani and I. Ghafir, "Optimisation de la couverture pour les réseaux sans fil aériens," 14e Conférence Internationale sur les Innovations en Technologie de l'Information (IIT), pp. 233–238, Nov. 2020.

[13] K. Singh and H. Gupta, "A new approach for the security of vpn," in *Second International Conference on Information and Communication Technology for Competitive Strategies*, Mar. 2016, pp. 1–5.

[14] M. Iqbal and I. Riadi, "Analysis of security virtual private network (vpn) using openvpn," *International Journal of Cyber-Security and Digital Forensics*, vol. 8, no. 1, pp. 58–65, 2019.

[15] A. Gaikar, *Le réseau privé virtuel (VPN) : Une technologie pour améliorer l'anonymat et la sécurité*, 2013.

[16] X. Lasserre, T. Klein *et al.* (2007) Réseaux privés virtuels vpn. Consulté le 05/06/2022. [Online]. Available : http://www.frameip.com/vpn

[17] P. Jean-François and B. Jean-Phillipe, *Tout sur la Sécurité informatique.* DUNOD, 2005.

[18] H. Mao, L. Zhu, and H. Qin, "A comparative research on ssl vpn and ipsec vpn," in *2012 8th International Conference on Wireless Communications, Networking and Mobile Computing*, 2012.

[19] F. Aparicio-Navarro, K. Kyriakopoulos, I. Ghafir, S. Lambotharan, and J. Chambers, "Multi-stage attack detection using contextual information," in *MILCOM 2018.* IEEE, Oct. 2018.

[20] Ipsec explained : what it is and how it works. [Online]. Available : https://www.cloudns.net/blog/ipsec-explained-what-it-is-and-how-it-works/

[21] Wireguard whitepaper. [Online]. Available : https://www.wireguard.com/papers/wireguard.pdf

[22] G. Pujolle, *Les Réseaux.* Eyrolles, 2000.

[23] W. Tay, S. Lew, and S. Ooi, "Remote access vpn using mikrotik router," in *2022 International Conference on Computer and Drone Applications (IConDA).* IEEE, Nov. 2022, pp. 119–124.

[24] Y. Shah and S. Sengupta, "A survey on classification of cyber-attacks on iot and iiot devices," in *2020 11th IEEE UEMCON.* IEEE, Oct. 2020, pp. 406–413.

[25] R. Bansode and A. Girdhar, "Common vulnerabilities exposed in vpn–a survey," in *Journal of Physics : Conference Series*, vol. 1714, no. 1. IOP Publishing, 2021, p. 012045.

[26] Vpn : dangers de l'utilisation. [Online]. Available : https://www.clubic.com/antivirus-securite-informatique/vpn/article-874693-1-danger-utilisation-vpn.html

[27] V. Remazeilles, *La sécurité des réseaux avec Cisco.* Edition ENI, 2009.

[28] Guide pratique : Les vpn, avantages et vulnérabilités. [Online]. Available : https://www.webcyber.co/guide-pratique-les-vpn-avantages-et-vulnerabilites/

[29] Vpn : Usage par les hackers, risques et précautions. [Online]. Available : https://cyberinstitut.fr/vpn-hackers-usage-risques-precautions/

[30] Les risques à connaître et les précautions à prendre sur les vpn gratuits. [Online]. Available : https://www.lesnumeriques.com/vpn/les-risques-a-connaitre-et-les-precautions-a-prendre-sur-les-vpn-gratuits-a227021.html

[31] Risques liés à l'utilisation d'un vpn gratuit. [Online]. Available : https://www.mozilla.org/fr/products/vpn/resource-center/risks-of-using-a-free-vpn/

[32] What is vpn monitoring. [Online]. Available : https://checkmk.com/guides/what-is-vpn-monitoring

[33] Vpn monitoring - paessler. [Online]. Available : https://www.paessler.com/vpn-monitor

[34] Surveillance réseau vpn - manageengine. [Online]. Available : https://www.manageengine.com/fr/network-monitoring/

[35] P. AG. (2023) Prtg network monitor – the all-in-one monitoring solution. [Online]. Available : https://www.paessler.com/prtg

[36] Nagios. [Online]. Available : https://www.nagios.com/

[37] Z. LLC, *Zabbix Documentation 6.4*, 2024.

[38] Wazuh, "Wazuh : Open source security platform," https://wazuh.com/, 2025.

[39] P. T. AG. (2023) Protonvpn - secure and private vpn service. [Online]. Available : https://protonvpn.com

[40] I. OpenVPN Technologies. (2023) Openvpn - a virtual private network (vpn) solution. [Online]. Available : https://openvpn.net

[41] H. VPN. (2023) Hola vpn – unblock websites and hide your ip. [Online]. Available : https://www.hola.org