République Algérienne Démocratique et Populaire
Ministère de l'enseignement Supérieur et de la Recherche Scientifique
Université Saad Dahleb Blida 1
Faculté des Sciences
Département d'Informatique

Mémoire de Fin D'Etudes

Pour l'Obtention
Du Diplôme de Master en Informatique
Option : Sécurité des systèmes informatiques (SSI)

Déploiement et test d'un pare-feu Fortinet

Toubal adel

Membres de jury :
Président :Mohamed Benyahia
Examinateur : Abdellah Kameche
Promoteur : Mohamed Ould-Khaoua
Encadreur : Bellil Omar

2021/2022

Résumé

De nos jours, la sécurité informatique est quasi-indispensable pour le bon fonctionnement d'un réseau, aucune entreprise ne peut prétendre vouloir mettre en place une infrastructure réseau, quel que soit sa taille, sans envisager une politique de sécurité. Nous avons tout au long de notre travail déploiement et test d'un pare-feu Fortinet. Le principe de notre travail est de mettre à la différence entre l'utilisation la configuration classique de firewall dans le monde réel, avec l'utilisation de la nouvelle génération de Firewall qui utilise la notion de IA pour nous facilite le travail, détection et utilisation de manière générale. Notre proposition peut permettre aux utilisateurs de gagner en simplification d'accès à leur application. Pour terminer, nous tenons à souligner que nous n'avons nullement pas la prétention d'avoir présenté. Comme perspectives de notre projet nous proposons :

- Utilisation la notion de la configuration de la sécurité de nos système classique avec les commandes, …etc.
- Utilisation de la nouvelle génération de firewall qui est fabriquer par le principe de IA.

Notre objectifs, c'est de faire configurer la Fortinet et son firewall pour etablir une securite dans l'entreprise. A la fin, nous avons accompli notre objetifs qui c'est de configurer notre Fortinet. D'ou, nous avons conclus que la plateforme de la fortinet nous facilite le configuration.

ملخص

في الوقت الحاضر، يكاد يكون أمن تكنولوجيا المعلومات ضروريًا للعمل السليم للشبكة، ولا يمكن لأي شركة أن تدعي أنها تريد إنشاء بنية تحتية للشبكة، مهما كان حجمها، دون التفكير في سياسة أمنية. لدينا طوال عملنا نشر واختبار جدار حماية Fortinet. مبدأ عملنا هو التمييز بين استخدام تكوين جدار الحماية التقليدي في العالم الحقيقي، مع استخدام الجيل الجديد من Firewall الذي يستخدم فكرة الذكاء الاصطناعي لتسهيل عملنا واكتشافنا واستخدامنا العام. يمكن أن يسهل اقتراحنا على المستخدمين الوصول إلى تطبيقاتهم. في الختام، نود أن نؤكد أننا لا ندعي أننا قدمنا أي تشريع. وكآفاق لمشروعنا، نقترح ما يلي:

- استخدام مفهوم تكوين أمن أنظمتنا التقليدية بضوابط، إلخ.
- استخدام توليد جدار الحماية الجديد المصنوع بمبدأ الذكاء الاصطناعي.

هدفنا هو تكوين Fortinet وجدار الحماية الخاص بها لتأسيس الأمن في الشركة. في النهاية، حققنا هدفنا المتمثل في تكوين Fortinet. وبالتالي، خلصنا إلى أن منصة fortinet تسهل التشكيل.

Dédicace

Je dédie ce modeste travail comme un témoignage d'affection, de respect et d'admiration :

A mes très chers parents,

Pour tout ce que vous avez fait pour moi, pour les efforts que vous avez consentis pour mon éducation et ma formation. Je ferai de mon mieux pour rester un sujet de fierté à vos yeux avec l'espoir de ne jamais vous décevoir.

A mon cher frère et sœur,

Pour votre présence dans ma vie, pour votre précieux soutien moral et matériel, pour vos encouragements continus, votre affection et vos soutiens m'ont été d'un grand secours au long de ma vie.

A toute la famille **TOUBAL** et la famille **BOUKHELKHAL**,

L'expression de mes sentiments de respect et de reconnaissance pour le soutien qu'ils n'ont cessé de me porter.

A mes chers Amis,

Pour votre amitié, pour les meilleurs souvenirs, pour les bons moments, pour l'encouragement et le soutien.

A mes enseignants, Pour votre aide tout au long de mon cursus scolaire, je serai toujours reconnaissante.

A tous ceux que j'aime et à tous ceux qui m'aiment.

TOUBAL Adel.

Remerciement

Je rends grâce à Dieu, le miséricordieux, de nous avoir donnée la force, la volonté et la patience pour pouvoir accomplir ce modeste travail.

Toute notre reconnaissance et toute notre gratitude vont vers notre promoteur de la société **LogiTrans**, qui nous a aidé et accompagné tout au long de cette expérience professionnelle avec beaucoup de patience et d'enthousiasme.

Nos profonds remerciements s'adressent à Mr **Mohamed Ould-Khaoua**, notre enseignante à l'université, de nous avoir guidé et orienté durant les différentes étapes de ce projet avec sa pédagogie et ¸sa ferveur.

Nous remercions également les membres du jury d'avoir accepté d'examiner et de juger notre travail.

Que tous ceux qui, de près ou de loin ont contribué, par leurs conseils, leurs encouragements ou leur amitié à l'aboutissement de ce travail, trouvent ici l'expression de ma profonde reconnaissance.

Pour leur encouragement, leur soutien moral et la patience qu'ils nous ont manifestée durant toute l'année, nous remercions fortement tous les membres de ma famille.

Enfin remercier mes parents serait se répéter, parfois pour exprimer plus que ce qu'on a envie de dire on a recours au silence.

Table des matières

Liste des Abréviations

DMZ	Zone demilitarisee
DHCP	Dynamic Host Configuration Protocol
IP	Internet Protocol
NAT	Network Adress Translation
PAT	Port Adress Translation
SSL	Secure Sockets Layer
DNS	Domain Name System
LAN	Local Area Network
WAN	Wide Area Network
IDS	Intrusion Detection System
IPS	Intrusion Prévention System
PME	Petites et Moyennes Entreprises
TCP	Transmission Control Protocol
ARP	Address Resolution Protocol
DOS	Denial Of Service
DDOS	Distributed Denial Of Service

Liste des Figures

Introduction générale

Le réseau informatique désigne les appareils informatiques interconnectés qui peuvent échanger des données et partager des ressources entre eux. Ces appareils en réseau utilisent un système de règles, appelées protocoles de communication, pour transmettre des informations sur des technologies physiques ou sans fil [20].

À une époque où communication et technologie sont les maîtres mots de notre société, on ne peut douter que l'avenir des réseaux informatiques soit de grandir et de se développer. Cet avenir est pour une bonne partie lié aux techniques et aux supports de communication utilisés dans les réseaux. De plus, la technologie actuelle permet d'accroître les volumes et les débits de transfert de données tout en diminuant les coûts. Les interconnexions des réseaux sont variées et pratiquement tous se trouvent aujourd'hui imbriqués les uns dans les autres.

Pour parer à ces attaques, une architecture sécurisée est nécessaire. Pour cela, le cœur d'une telle architecture est basé sur un firewall. Cet outil a pour but de sécuriser au maximum le réseau local de l'entreprise, de détecter les tentatives d'intrusion et d'y parer au mieux possible. Cela représente une sécurité supplémentaire rendant le réseau ouvert sur Internet beaucoup plus sûr. De plus, il peut permettre de restreindre l'accès interne vers l'extérieur. En effet, des employés peuvent s'adonner à des activités que l'entreprise ne cautionne pas. En plaçant un firewall limitant ou interdisant l'accès à ces services, l'entreprise peut donc avoir un contrôle sur les activités se déroulant dans son enceinte.

Dans ce mémoire nous décrivons le déploiement et test d’un pare-feu Fortinet. Comme une étude de cas, cette dernière est appliquée au réseau de la société LogiTrans. Ainsi, nous avons optés pour une mise en place d’une architecture réseau sécurisé pour que l’accessibilité à l’information soit immédiate à n’importe quel moment et n’importe quel endroit.

Nous avons organisée mémoire en quatre chapitres. Dans le premier nous allons introduire le concept général sur la sécurité des systèmes informatiques.

Dans le deuxième chapitre, nous expliquerons la Fortinet.

Dans le troisième chapitre, nous décrivons à l’environnement Simulation.

Le quatrième chapitre sera consacré à l’aspect pratique du pare-feu Fortinet.

Enfin, nous terminons notre mémoire par une conclusion et une bibliographie.

Chapitre 01 :

Concepts générales sur la sécurité des systèmes informatiques

1.1 Introduction

Dans ce chapitre nous allons présenter quelques concepts généraux des pare-feus ainsi que la zone démilitarisée (De-Militarized Zone (DMZ)) et leurs avantages dans notre travail réalise et aussi les pare-feus sur le système d'exploitation Windows et aussi les pare-feu open-source et à la fin, une présentation préliminaire sur le pare-feu Fortinet.

1.2 Concept du pare-feu

Un pare-feu (*firewall*) protège des tentatives de connexion directe venant d'un réseau comme Internet. Par contre, il laisse entrer le retour légitime du trafic initié d'une zone de confiance comme un LAN. Il tient compte de l'état des sessions de couche 4 établies (TCP, UDP, ICMP, etc.). On parle alors de pare-feu à état. Figure 1 et figure 2 présente les symboles pare-feu firewallet la topologie pare-feu avec DMZ[1].

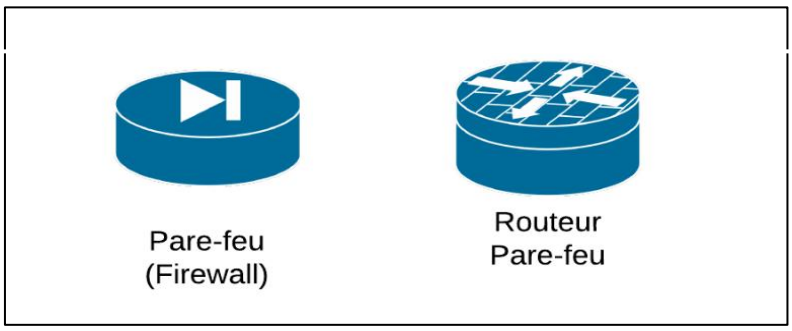

Figure 1 : Symboles d'un pare-feu (firewall).

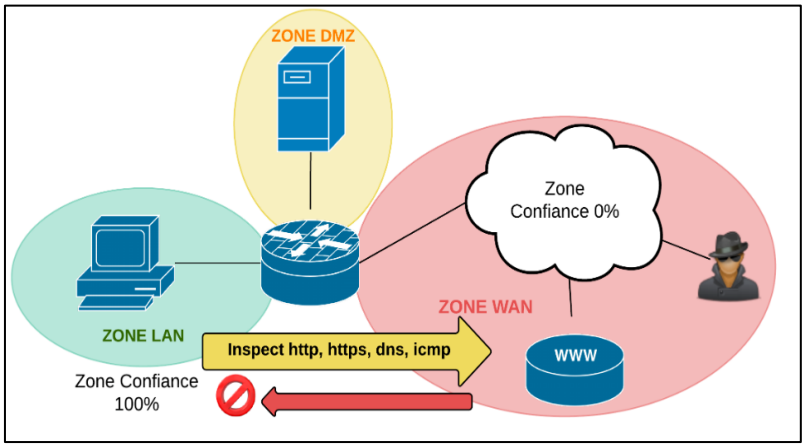

Figure 2 : Topologie pare-feu avec DMZ.

Quelques éléments essentiels à retenir surle Pare-feu

Dans un système d'information, les politiques de filtrage et de contrôle du trafic sont placées sur un matériel ou un logiciel intermédiaire communément appelé pare-feu. Cet élément du réseau a pour fonction d'examiner et filtrer le trafic qui le traverse. On peut le considérer comme une fonctionnalité d'un réseau sécurisé : la fonctionnalité pare-feu, L'idée qui prévaut à ce type de fonctionnalité est le contrôle des flux du réseau TCP/IP. Le pare-feu limite le taux de paquets et de connexions actives. Il reconnaît les flux applicatifs. Se placer au milieu du routage TCP/IP, il fait office de routeur, Il agit au minimum au niveau de la couche 4 (L4)

mais il peut inspecter du trafic L7 (Web Application Firewall). Il ne faut pas le confondre avec le routeur NAT [1].

1.3 Objectifs d'un pare-feu

Un pare-feu a pour objectifs de répondre aux menaces et attaques suivantes, de manière non-exhaustive :

- Usurpation d'identité.
- La manipulation d'informations.
- Les attaques de déni de service (DOS /DDOS).
- Les attaques par code malicieux.
- La fuite d'information.
- Les accès non-autorisé (en vue d'élévation de privilège).
- Les attaques de reconnaissance, d'homme du milieu, l'exploitation de TCP/IP [1].

1.4 Ce que le pare-feu ne fait pas

Le pare-feu est central dans une architecture sécurisée mais :

- Il ne protège pas des menaces internes.
- Il n'applique pas tout seul les politiques de sécurité et leur surveillance.
- Il n'établit pas la connectivité par défaut.
- Le filtrage peut intervenir à tous les niveaux TCP/IP de manière très fine.

1.5 Fonctionnement d'un pare-feu

Il a pour principale tâche de contrôler le trafic entre différentes zones de confiance, en filtrant les flux de données qui y transitent.

Généralement, les zones de confiance incluent l'Internet (une zone dont la confiance est nulle) et au moins un réseau interne (une zone dont la confiance est plus importante). Le but est de fournir une connectivité contrôlée et maîtrisée entre des zones de différents niveaux de confiance, grâce à l'application de la politique de sécurité et d'un modèle de connexion basé sur le principe du moindre privilège. Un pare-feu fait souvent office de routeur et permet ainsi d'isoler le réseau en plusieurs zones de sécurité appelées zones démilitarisées ou DMZ. Ces zones sont séparées suivant le niveau de confiance qu'on leur porte [1].

1.6 Zone de confiance sur un pare-feu

Une organisation du réseau en zones composées d'interfaces permet d'abstraire les règles de filtrages. Voir la figure 3.

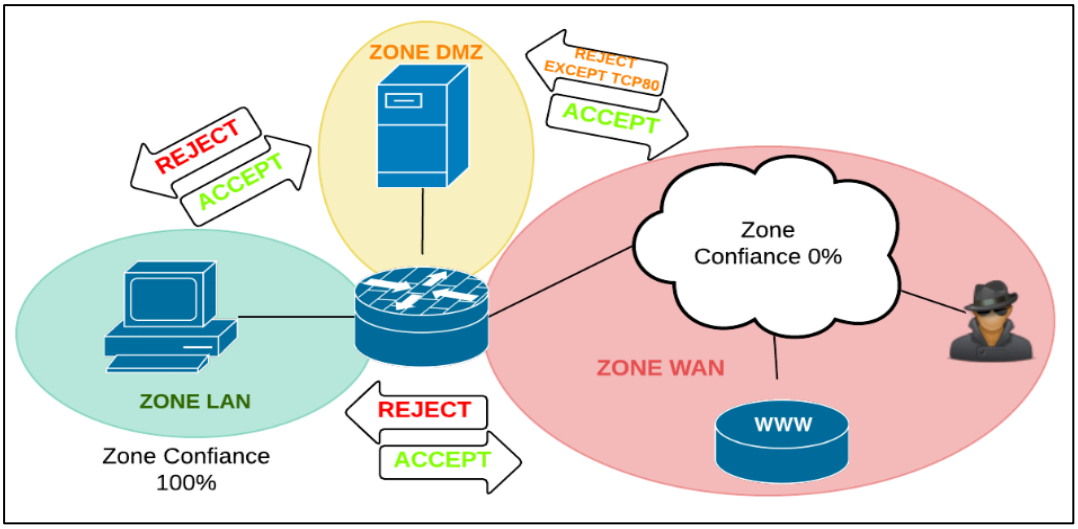

Figure 3 : Zones de confiance.

À titre d'exemple, les politiques de filtrage des applications pourraient être facilement mis en œuvre quel que soit le protocole de transport IPv4 ou IPv6. Aussi les politiques de sécurité appliquée sur les pare-feu sont alors plus lisibles, plus faciles à auditer et à gérer [1].

1.7 Niveau de confiance

Le niveau de confiance est la certitude que les utilisateurs vont respecter les politiques de sécurité de l'organisation. Ces politiques de sécurité sont édictées dans un document écrit de manière générale. Ces recommandations touchent tous les éléments de sécurité de l'organisation et sont traduites particulièrement sur les pare-feu en différentes règles de filtrage. On notera que le pare-feu n'examine que le trafic qui le traverse et ne protège en rien des attaques internes, notamment sur le LAN.

1.8 Filtrage

Selon les besoins, on placera les politiques de filtrage à différents endroits du réseau, au minimum sur chaque hôte contrôlé (pare-feu local) et en bordure du réseau administré sur le pare-feu. Ces emplacements peuvent être distribué dans la topologie selon sa complexité. Pour éviter qu'il ne devienne un point unique de rupture, on s'efforcera d'assurer la redondance des pare-feu. On placera plusieurs pare-feu dans l'architecture du réseau à des fins de contrôle au plus proche d'une zone ou pour répartir la charge.

La configuration d'un pare-feu consiste la plupart du temps en un ensemble de règles qui déterminent une action de rejet ou d'autorisation du trafic qui passe les interfaces du pare-feu en fonction de certains critères tels que : l'origine et la destination du trafic, des informations d'un protocole de couche 3 (IPv4, IPv6, ARP, etc.), des informations d'un protocole de couche 4 (ICMP, TCP, UDP, ESP, AH, etc.) et/ou des informations d'un protocole applicatif (HTTP, SMTP, DNS, etc.).

1.9 Les différents types de filtrage

- Filtrage simple des paquets (ACL).
- Passerelles au niveau du circuit.
- Pare-feu d'inspection avec état.
- Filtrage applicatif (ou pare-feu de type proxy ou proxy applicatif).
- Pare-feu nouvelle génération.

Règle :

Chaque règle est examinée selon son ordonnancement. Si le trafic ne correspond pas à la première règle, la seconde règle est évaluée et ainsi de suite. Lorsqu'il y a correspondance entre les critères de la règle et le trafic, l'action définie est exécutée et les règles suivantes ne sont pas examinées. La terminologie des actions usuelles peut être accepté, permit, Denny, block, rejet, drop, ou similaires.

En général, un ensemble de règles se termine par le refus de tout trafic, soit en dernier recours le refus du trafic qui traverse le pare-feu. Ce comportement habituellement défini par défaut ou de manière implicite refuse tout trafic pour lequel il n'y avait pas de correspondance dans les règles précédentes. [1]

1.10 Type de pare-feu :

1- Les pare-feu avec des câbles réseau : avec la fonction de filtrage en plus. Leurs interfaces ne possèdent Les pare-feu bridge, Ces derniers sont relativement répandus. Ils agissent comme pas d'adresse IP, et ne font que transférer les paquets d'une interface a une autre en leur appliquant les règles prédéfinies. Cette absence est particulièrement utile, car cela signifie que le firewall est indétectable. Par ailleurs, ces derniers ont une interface de configuration séparée. Un câble vient se brancher sur une troisième interface, série ou Ethernet [2].

2- Les pare-feu matériels : il s'agit d'un équipement physique conçu pour effectuer des tâches de pare-feu. Un pare-feu matériel peut être un ordinateur ou un équipement dédié qui sert de pare-feu. Le pare-feu matériel est intégré au routeur situé entre l'ordinateur et la passerelle Internet [2].

3- Les pare-feu logiciels : est un type spécial de logiciel informatique exécuté sur un ordinateur/serveur. Son objectif principal est de protéger votre ordinateur/serveur des tentatives extérieures de contrôle ou d'accès et en fonction de votre choix de pare-feu logiciel. Le pare-feu logiciel peut également être configuré pour vérifier toutes les demandes sortantes suspectes.

1.11 Pare-feu sur Windows

Lorsque vous êtes connecté à Internet, des données sont échangées entre votre PC et les serveurs qui hébergement les sites web et les services web que vous consultez/utilisez. Ces échanges forment ce que l'on appelle le **trafic réseau**. On distingue le **trafic réseau entrant** pour les connexions reçues depuis Internet vers votre PC, et le **trafic réseau sortant** pour les connexions émises depuis votre PC vers Internet. Le pare-feu permet de **contrôler ce trafic réseau**, il est ainsi en mesure d'autoriser ou bloquer les connexions

entrantes et sortantes sur votre PC. Concrètement, le pare-feu vous permet de **contrôler l'activité de votre PC** en autorisant ou en bloquant les applications qui demandent l'accès à Internet (demande de connexion entrante ou sortante), vous permettant ainsi de **protéger votre PC des infections et des intrusions** venant d'Internet. Nous allons donc explorer la liste des meilleurs programmes de pare-feu Windows 10 que vous pouvez utiliser sur votre système[3].

1.11.1 COMODO FIREWALL

COMODO Firewall est l'un des meilleurs outils de pare-feu Windows gratuits que vous pouvez utiliser sur votre ordinateur Windows 10. L'interface de COMODO Firewall est très propre et très facile à utiliser. Il vous suffit d'ajouter des programmes à la liste de blocage pour limiter l'utilisation d'Internet. COMODO Firewall propose également un bloqueur de publicité, des serveurs DNS personnalisés et un mode de jeu.la figure 4 est leur interface[4].

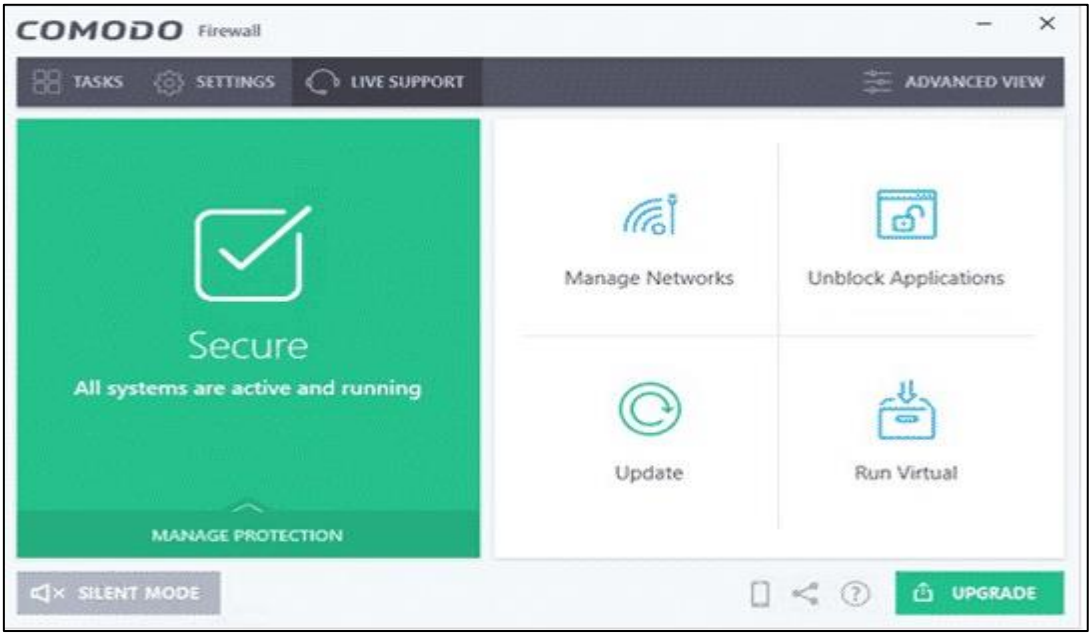

Figure 4 : COMODO FIREWALL.

1.11.2 TIMY WALL

Si vous recherchez un programme de pare-feu pour votre ordinateur Windows 10 qui n'envoie pas de notifications inutiles, TINY WALL est peut-être le meilleur choix pour vous. Le programme de pare-feu est connu pour son interface légère et propre et permet aux utilisateurs de sélectionner des applications pour lui attribuer manuellement des autorisations de pare-feu. TINY WALL est donc un autre meilleur programme de pare-feu que vous pouvez utiliser sur votre ordinateur Windows 10. Voire figure 5 [4].

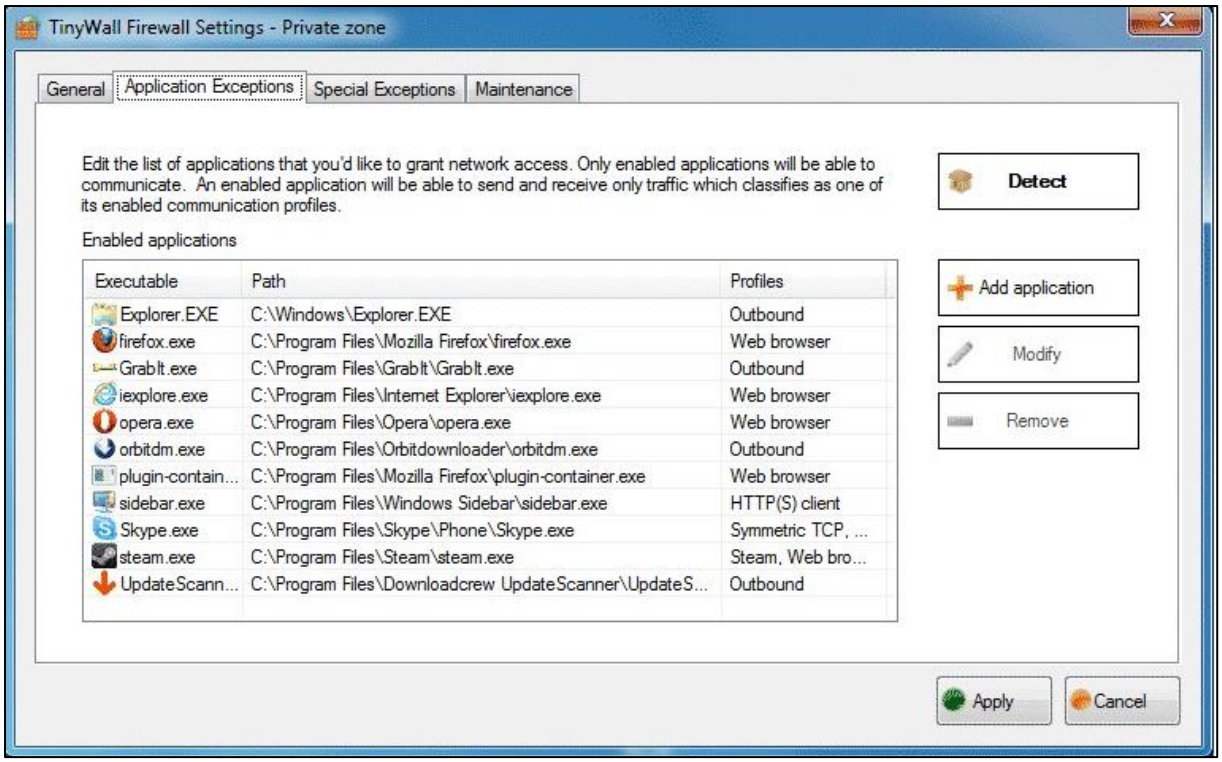

Figure 5 : TINY WALL FIREWALL.

1.11.3 ZONE ALARME FREE FIREWALL

ZONE ALARME, le principal fabricant d'antivirus, dispose également d'un outil de pare-feu gratuit qui permet aux utilisateurs d'ajuster le mode de sécurité des réseaux publics et privés. Le programme de pare-feu propose deux types de sécurité Auto-LEARN ou Max Security. La fonctionnalité Apprentissage automatique apporte des modifications en fonction de votre comportement et Max Security offre aux utilisateurs la possibilité de contrôler chaque application manuellement. Le programme de pare-feu propose également un mode de jeu qui bloque les notifications pendant le jeu. Figure 6 [4].

Figure 6 : ZONE ALARME FIREWALL.

1.11.4 PEER BLOCK

PEER BLOCK est un peu différent de tous les autres programmes de pare-feu Windows répertoriés dans l'article. Au lieu de programmes bloquants, PEER BLOCK bloque la liste des adresses IP appartenant à des catégories spécifiques. Par exemple, il peut charger et bloquer la liste des adresses IP identifiées comme fournisseurs d'entreprise, éducation, annonces, logiciels espions, P2P, etc. PEER BLOCK est donc un autre meilleur programme de pare-feu Windows que vous pouvez utiliser maintenant. Voire figure 7 [4].

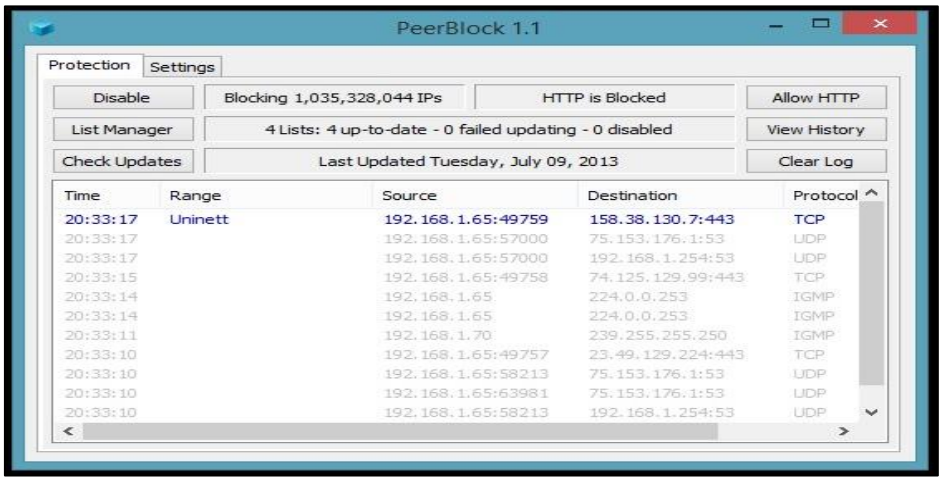

Figure 7 : PEER BLOCK FIREWALL.

1.11.5 AVS FIREWALL

Si vous recherchez un outil de pare-feu Windows pour bloquer les modifications de registre, les fenêtres contextuelles, les bannières flash, les annonces, etc. malveillants, AVS Firewall est sans doute le meilleur choix pour vous. AVS Firewall peut empêcher les programmes, l'adresse IP et les ports d'accéder à votre connexion Internet. L'interface utilisateur est un autre aspect positif de cet outil, et le programme est compatible avec presque toutes les versions de Windows. Voir figure 8 [4].

Figure 8 : AVS FIREWALL.

1.11.6 OUT PORT FIREWALL

OUT PORTFirewall est un autre meilleur programme de pare-feu Windows de la liste qui peut considérablement améliorer le niveau de sécurité de votre système. Le point fort de OUT PORT Firewall est qu'il dispose d'un algorithme d'auto-apprentissage capable de détecter des programmes partageant certaines similitudes. Par exemple, si vous utilisez un enregistreur d'écran sur votre ordinateur et si vous lui avez attribué des autorisations de pare-feu, OUT PORT Firewall empêchera automatiquement les autres enregistreurs d'écran d'utiliser Internet [4].

Figure 9 : OUT POST FIREWALL.

1.11.7 R-FIREWALL

R-Firewall est l'un des programmes de pare-feu Windows les plus avancés que vous aimeriez utiliser aujourd'hui. Cependant, le programme n'est pas très facile à utiliser car son interface regorge de paramètres et d'options. Cependant, R-Firewall est capable d'exécuter des tâches avancées telles que le blocage des publicités, du javascript, des suivis Web, des mots-clés, des filtres de messagerie, etc. Ainsi, R-Firewall est le programme de pare-feu le plus avancé que vous puissiez utiliser actuellement. Voire figure 10 [4].

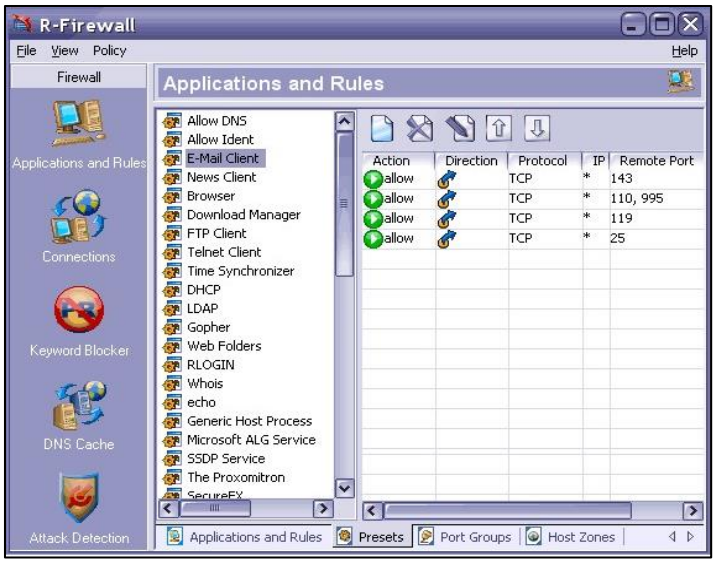

Figure 10 : R-Firewall.

Voici donc les huit meilleurs programmes de pare-feu que vous pouvez utiliser sur votre ordinateur Windows 10.

1.11.8 NET DEFENDER

Si vous recherchez un programme pare-feu simple à utiliser mais efficace pour votre ordinateur Windows 10, alors NET DEFENDERest sans doute le meilleur choix pour vous. Le programme permet aux utilisateurs de définir une adresse IP source et de destination, un numéro de port, un protocole pour bloquer ou autoriser n'importe quelle adresse. Non seulement cela, mais NET DEFENDERa également un scanner de ports qui peut voir quels ports sont ouverts sur votre système. Est donc un autre programme de pare-feu efficace que vous pouvez utiliser aujourd'hui. Voir figure 11. [4]

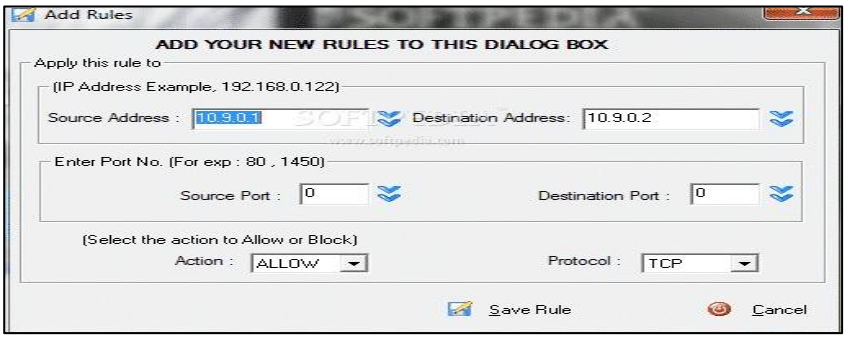

Figure 11 : NET DEFENDER FIREWALL.

1.12 Pare-feu open source

Les programmes open source offrent aux utilisateurs professionnels et individuels la possibilité de configurer toutes les fonctions essentielles du réseau pour un fonctionnement correct. En bref, il existe des solutions qui permettent la configuration des fonctions de routage et des réseaux en général, comme DHCP et DNS. Revenons à la mention de la sécurité, ces programmes open-source disposent de plusieurs fonctionnalités qui permettent

d'ajouter un bouclier de protection considérable : pare-feu, antivirus, services antispam et filtres web. Voici les meilleurs pare-feu open-source [5].

1.12.1 Pf-sensé

Il s'agit d'une solution de pare-feu open source basée sur FreeBSD, elle dispose d'un noyau personnalisé, qui peut être installé sur la machine de votre choix. Cependant, vous pouvez opter pour l'alternative de monter une machine virtuelle (VMWare, Virtual Box et autres) et d'installer Pf-sensé en utilisant l'Image ISO. De plus, grâce aux machines virtuelles, il est également possible d'installer via un périphérique USB amorçable ou l'image intégrée (.**IMG**). Voir figure 12 [5].

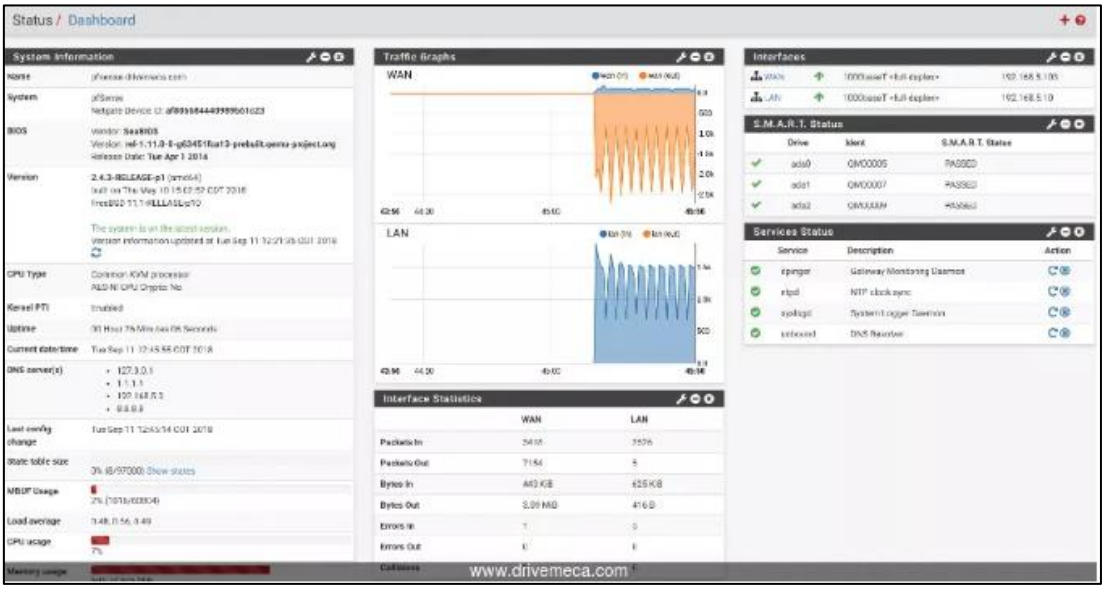

Figure 11 : Pf-sensé pare-feu open source.

Voici quelques fonctionnalités :

- Fonctions avancées de routage et de pare-feu.
- NAT (Network Adresse Translation), mieux connu sous le nom de NATEO.
- Équilibreur de charge.
- Il a un client / serveur VPN avec IP-sec et Open-VPN.
- Surveillance avancée de l'activité du réseau à l'aide de journaux et de graphiques.
- Serveur DNS.
- Systèmes IDS / IPS avec Suricate pour protéger davantage le réseau
- DNS dynamique et portails captifs.
- Services de relais DHCP et DCHP.
- Possibilité d'installer des logiciels supplémentaires pour avoir plus de services disponibles.

1.12.2 IP-FIRE

Il est considéré comme l'une des meilleures solutions de pare-feu open source. Il se caractérise par sa modularité et sa grande flexibilité dès le début de sa conception. Il a non

seulement des fonctions de pare-feu, mais aussi en tant que **le serveur proxy** et passerelle VPN[5].

D'autre part, il dispose d'un système IDS qui analyse le trafic réseau pour trouver les vulnérabilités potentielles et leurs exploits. Cela signifie que si une attaque est détectée, l'événement et son auteur seront bloqués. Voire figure 12 [5].

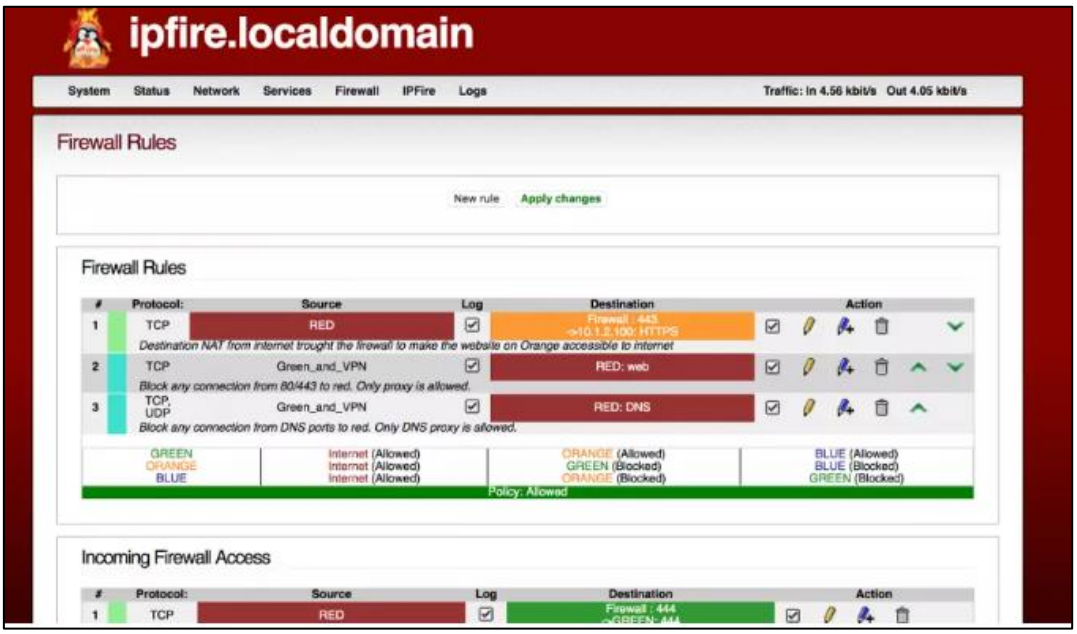

Figure 12 : IP-FIRE firewall open source.

De plus, le fait que vous ayez accès au code source permet une grande transparence et permet aussi de s'assurer qu'il n'y a rien de malveillant et que tout est normal**.** Les solutions Open Source permettent d'accéder beaucoup plus rapidement à l'innovation. Les solutions Open Source ne sont pas monolithiques, elles sont en fait très modulables [5].

1.13 Pare-feu Fortinet

Fortinet fournit des solutions de sécurité haute performance qui protègent votre réseau, vos utilisateurs et vos données contre des menaces en évolution permanente. Notre gamme étendue de solutions de sécurité et de plateformes de gestion centralisée permet de consolider la sécurité et de simplifier l'infrastructure de sécurité. Voir Figure 13 [6].

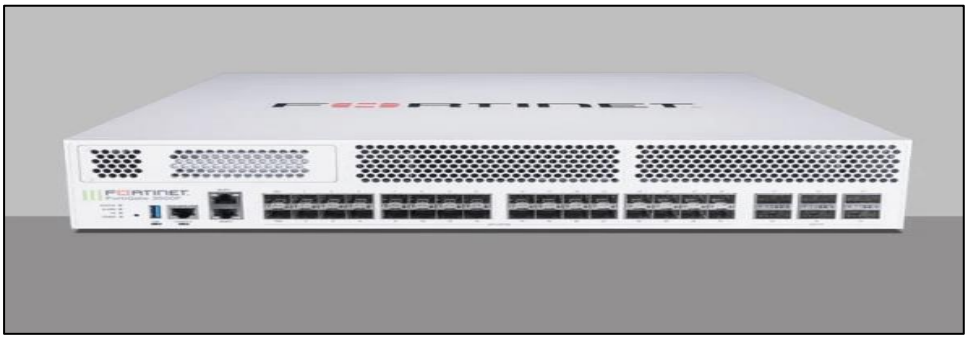

Figure 13 : pare-feu haute performance de nouvelle génération.

1.13.1 Les pare-feux de nouvelle génération (NGFW)

Filtrent le trafic réseau d'une entreprise pour la protéger des menaces internes et externes. Ils reprennent à leur compte les fonctionnalités des pare-feux Stateful : filtrage de paquets, inspection du trafic IPSEC et des VPN sous SSL, monitoring réseau ou encore les fonctions de mapping IP. Et ils vont au-delà grâce à des fonctions plus pointues d'inspection des contenus. Ces fonctionnalités permettent d'identifier les assaillants, les malwares et autres menaces, qui seront ainsi neutralisées par le pare-feu NGFW. Les entreprises bénéficient d'une inspection SSL, d'un contrôle applicatif, d'une prévention des intrusions et d'une visibilité précise sur l'ensemble de la surface d'attaque. Alors que l'univers des menaces évolue et s'adapte à la migration vers le Cloud et l'adoption du multicloud par les entreprises, et que ces dernières doivent répondre à des besoins clients toujours plus exigeants, les pare-feux traditionnels peinent à tenir le rythme et à proposer une protection évolutive. Il en résulte un fort impact sur l'expérience des utilisateurs et sur le niveau de sécurité. Les NGFW ne se contentent pas de neutraliser les malwares. Ils sont conçus pour être mise à jour, ce qui leur permet de suivre l'évolution des menaces et de pérenniser la protection du réseau face aux nouvelles menaces. Le pare-feu de nouvelle génération devient ainsi une pièce maîtresse pour déployer la sécurité réseau [23].

1.13.2 Gestion des risques internes de sécurité

Compte tenu de la forte croissance du trafic HTTPS, les entreprises qui ne disposent pas de stratégies de déchiffrement TLS n'ont aucune visibilité sur près de 90% de ce trafic qui est chiffré. Elles s'exposent ainsi à des campagnes de malware ciblées et à des pertes de données. FORTIGATE offre des fonctions réseau orientées sécurité pour déployer une visibilité intégrale au cœur des applications, des menaces et des réseaux. Le pare-feu protège ainsi tous les Edge réseau en leur appliquant une sécurité éprouvée qui pérennise l'activité opérationnelle et assure la continuité métier [24].

1.13.3 Gestion des risques externes de sécurité

Les réseaux à plat sont plus vulnérables car ils ne bénéficient pas de fonctions d'inspection sophistiquée. FORTIGATE assure une segmentation du réseau pour limiter la surface d'attaque et freiner la propagation d'un assaillant sur le réseau. Les méthodes de segmentation (micro ou macro, basée sur les ports ou basée sur les applications) bénéficient de workflows automatisés, d'un niveau de confiance qui s'adapte et d'une protection haute performance contre les menaces, pour ainsi favoriser la conformité aux règles en vigueur et instituer un accès de confiance aux applications [24].

1.13.4 Gestion des vulnérabilités

La majorité des malwares se propage à l'aide de vulnérabilités connues qui sont des vecteurs d'attaque. Les pare-feux NGFW FORTIGATE offrent un IPS consolidé et sans impact sur les performances, ainsi qu'un rapiéçage virtuel, une prévention des attaques connues ou jour zéro, et une maîtrise des coûts et de la complexité [24].

1.13.5 Une sécurité à l'échelle HYPERSCALE

Les pare-feux traditionnels peinent à traiter rapidement le volume important du trafic utilisateur. Et c'est l'expérience utilisateur qui en subit les conséquences. La sécurité laisse

alors les assaillants s'infiltrer et mettre vos services en péril. Les NGFW de Fortinet déploient une sécurité unique et optimale pour s'assurer que vos sites Web restent accessibles, réactifs et garants d'une expérience utilisateur positive [7].

1.13.6 Sécurité les HUBS ON-RAMP vers le CLOUD

Les entreprises veulent bénéficier des avantages du Cloud en matière d'agilité, de résilience et d'évolutivité à la demande. Sécuriser et fluidifier le transfert de données vers et à partir du Cloud s'impose pour optimiser l'expérience utilisateur et assurer la conformité. Les pare-feux traditionnels ne permettent pas de transférer rapidement des volumes importants de données, ce qui, in fine, ralentit l'activité métier. En revanche, ces transferts rapides sont parfaitement gérés par les pare-feux de nouvelle génération Fortinet. Ceci est le cas pour les Eléphant Flows, à savoir ces ensembles importants de données (jusqu'à 100 Go) et chiffrés par IP sec. Accompagner les activités de recherche avec FORTIGATE 1800F. La sécurité laisse alors les assaillants s'infiltrer et mettre vos services en péril. Les NGFW de Fortinet déploient une sécurité unique et optimale pour s'assurer que vos sites Web restent accessibles, réactifs et garants d'une expérience utilisateur positive [8].

1.14 Pare-feu CISCO

Cisco Secure Firewall est un élément fondamental de la plateforme de sécurité ouverte la plus complète du marché. Pour protéger vos réseaux contre des menaces toujours plus sophistiquées, vous avez besoin d'informations de pointe et de protections cohérentes partout. Renforcez votre sécurité dès aujourd'hui avec Cisco Secure Firewall. Voir figure 14 [25].

Figure 14 : Pare-feu de nouvelle génération Cisco FIRE-POWER 1000 - Cisco.

1.14.1 Pare-feu de nouvelle génération Cisco FIRE-POWER 1000 - Cisco

Les pare-feu FIRE-POWER série 1000 offrent les performances, la facilité d'utilisation et le niveau avancé de visibilité et de contrôle nécessaires pour détecter et stopper rapidement les menaces. Ils ont été conçus pour optimiser les services de sécurité sans nuire aux performances du réseau [9].

1.14.2 Contrôles de sécurité performants

Pour sécuriser votre réseau contre des menaces toujours plus sophistiquées, vous avez besoin d'informations de premier ordre et d'une protection globale parfaitement uniforme. Renforcez votre sécurité dès aujourd'hui avec Cisco Secure Firewall [9].

1.14.3 Politiques et visibilités cohérentes

Les réseaux étant de plus en plus interconnectés, il est difficile de profiter d'une visibilité totale sur les menaces et d'assurer une gestion cohérente des politiques. Simplifiez la gestion de la sécurité et bénéficiez d'une visibilité sur tous les réseaux distribués et hybrides [9].

1.14.4 Intégration du réseau et de la sécurité

Cisco Secure Firewall pose les bases de l'intégration des fonctionnalités puissantes de prévention des menaces dans votre infrastructure de réseau. Votre réseau devient alors une extension logique de votre pare-feu [9].

Bénéficiez d'une gestion unifiée des pare-feux, du contrôle des applications, de la prévention des intrusions, du filtrage des URL et de la protection contre les malwares avancés. Profitez d'une configuration et d'une gestion locale simple du pare-feu pour les déploiements Cisco Secure Firewall de petite envergure [9].

1.15 Comparaison entre Fortiget et Cisco ASA

Déploiement	Fonctionnalités	Tarification
Cependant, si vous n'avez pas d'expérience dans l'utilisation de leurs produits, cela peut être complexe. En revanche, les utilisateurs de Fortinet Fortigate s'accordent à dire que le déploiement est facile et que la configuration initiale est simple.	Les examinateurs des deux solutions louent leur stabilité. Les fonctionnalités précieuses du pare-feu Cisco ASA incluent la détection et la prévention des intrusions, le contrôle des applications, le filtrage des URL, l'interface de ligne de commande, de bons rapports, une excellente visibilité, le VPN distant, l'ACL et l'accès basé sur les rôles. Certaines des fonctionnalités qui manquent aux utilisateurs incluent un meilleur cryptage, une interface utilisateur moins écrasante, un routage basé sur des politiques plus puissant et une meilleure configuration.	Les utilisateurs de Cisco ASA Firewall disent que le prix est élevé. Les utilisateurs de Fortinet Fortigate partagent des opinions mitigées, certains utilisateurs exprimant qu'ils pensent que le prix est abordable et juste et certains utilisateurs mentionnant qu'ils pensent que c'est du côté le plus cher.

Sur la base des paramètres que nous avons comparés, Fortinet Fortigate arrive en tête. Sa facilité de déploiement combinée à son ensemble solide de fonctionnalités et à ses excellentes notes de service et de support en fait une solution plus souhaitable que le pare-feu Cisco ASA.

1.16 Conclusion

Nous avons abordé dans ce chapitre quelque explication générale de notre travail.

On a commencé par une introduction dans le firewall et ces objectifs, le fonctionnement d'une façon général, la zone de confiance sur un pare-feu, niveau de confiance, le filtrage et différents types de filtrage. Les types de pare-feu sur windows, open source, Fortinet et Cisco. Apres cette comparaison, on travail avec la Fortinet.

Dans le chapitre qui suit nous allons expliquer quelque apprentissage automatique en utilisant le Fortinet.

Chapitre 02 :

Fortinet

2.1 Introduction

Dans cette chapitre on introduit la Fortinet on donne un aperçu de son histoire, la protection des données, les modèles et son spécification de chaque Fortiget, et la fin la cause de notre choix la Fortinet.

2.2 Fortinet

Fortinet est une multinationale américaine dont le siège social se situe à Sunnyvale (Californie). Elle conçoit et commercialise, entre autres, des logiciels, équipements (appliances) et services de cyber sécurité tels que des pare-feux, anti-virus, systèmes de prévention d'intrusion et de sécurité des terminaux. Elle occupe le quatrième rang mondial des acteurs de la sécurité réseau quant au chiffre d'affaires.

Fortinet a été créée en 2000 par les frères Ken et Michael Xie. Elle a levé environ 93 millions US$ de fonds sur la période allant jusqu'à 2004, et lancé dix appliances FortiGate. 2004 a également marqué le début d'un litige récurrent entre Fortinet et Trend Micro, portant sur un brevet. L'entreprise est entrée en bourse en 2009 et a levé 156 millions US$ lors de cette opération. Tout au long des années 2000, Fortinet a diversifié sa gamme de produits en y intégrant des points d'accès WiFi, une technologie de sandbox et des solutions de sécurité de la messagerie électronique notamment. [10].

2.3 Histoire de la Fortinet

Fortinet a été créée à Sunnyvale (Californie) en 2000 par les frères Ken et Michael Xie. Les fondateurs avaient précédemment évolué dans des rôles de management chez NetScreen et ServGate respectivement. Initialement baptisée Appligation Inc., la société fut renommée Appsecure en décembre 2000 puis, plus tard, Fortinet, un nom inspiré de l'expression **« Fortified Networks »** signifiant réseaux fortifiés. Après deux années consacrées à la recherche et le développement, l'entreprise a commercialisé son premier produit en 2002.

Fortinet a levé 13 millions US$ de fonds privés entre 2000 et début 2003. Elle a bouclé un tour de table de 30 millions US$ supplémentaires en août 2003, puis de 50 millions US$ en mars 2004, ce qui porte le financement total à 93 millions US$. Selon Fortinet, son chiffre d'affaires a été décuplé entre 2002 et 2003. Son premier programme à l'intention du réseau de distribution a vu le jour en octobre 2003. Westcon Canada a commencé à distribuer les produits FortiGate au Canada en décembre 2003, suivie par Norwood Adam au Royaume-Uni en février 2004. Le programme revendeurs a été réorganisé en janvier 2006 sous le nom de **« SOC in a BOX »**. En 2004, Fortinet était déjà présente, via ses bureaux, en Asie, en Europe et en Amérique du Nord.

En octobre 2005, une étude réalisée par OpenNet a révélé que les appliances Fortinet étaient utilisées pour censurer Internet au Myanmar. Fortinet a déclaré que ses produits étaient vendus par des revendeurs tiers et qu'elle respectait les embargos américains, mais il existe des photos montrant un représentant commercial de Fortinet en compagnie du Premier Ministre birman [22].

2.4 Comment un pare-feu Fortinet protège-t-il les données ?

Les filtres de pare-feu conservent les données nuisibles en dehors de votre ordinateur. Certains des principaux risques contre lesquels les pare-feu protègent votre ordinateur incluent les portes dérobées, les attaques par déni de service (DoS), les macros, les connexions à distance, le spam et les virus.

Les portes dérobées sont des « portes » vers des applications présentant des vulnérabilités que les attaquants exploitent pour pénétrer à l'intérieur. Cela inclut les systèmes d'exploitation qui peuvent avoir des bogues que les pirates peuvent utiliser pour accéder à votre ordinateur.

Les attaques DoS sont exécutées lorsqu'un pirate demande l'autorisation de se connecter à un serveur, et lorsque le serveur répond, il ne peut pas trouver le système qui a fait la demande. Lorsque cela se répète encore et encore, le serveur est inondé et doit dépenser tellement d'énergie pour traiter la masse de demandes, le rendant incapable de répondre aux besoins des visiteurs légitimes. Dans certains cas, le serveur doit se déconnecter complètement. Certains pare-feu peuvent vérifier si les demandes de connexion sont légitimes et ainsi protéger votre réseau des attaques DoS.

Les macros font référence à des scripts exécutés par des applications pour automatiser des processus. Une macro peut contenir une série d'étapes dépendantes qui sont toutes lancées par une seule commande. Les pirates conçoivent ou achètent des macros destinées à fonctionner dans certaines applications. Une macro peut être cachée dans des données apparemment innocentes, et une fois qu'elle entre dans votre ordinateur, elle fait des ravages sur votre système. Un pare-feu peut détecter des macros malveillantes lorsqu'il examine les paquets de données qui tentent de les traverser.

Les connexions à distance sont souvent utilisées pour aider une personne ayant un problème informatique. Cependant, entre les mains de la mauvaise personne, ils peuvent être abusés, en particulier parce que les connexions à distance offrent un accès presque complet à votre système.

Le spam peut parfois inclure des liens vers des sites Web malveillants. Ces types de sites activent un code malveillant qui force les cookies sur un ordinateur. Les cookies créent des portes dérobées permettant aux pirates d'accéder à l'ordinateur. Empêcher une attaque de spam est souvent aussi simple que de ne pas cliquer sur quoi que ce soit de suspect dans un e-mail, quel que soit l'expéditeur. Un pare-feu peut inspecter vos e-mails et empêcher votre ordinateur d'être infecté.

Les virus, une fois sur un ordinateur, se copient et se propagent sur un autre appareil du réseau. Les virus peuvent être utilisés pour faire une variété de choses, allant d'une activité relativement inoffensive à l'effacement de données sur votre ordinateur. Les pare-feu peuvent inspecter les paquets de données à la recherche de virus, mais il est préférable d'utiliser un logiciel antivirus en conjonction avec un pare-feu pour maximiser votre sécurité [28].

2.5 Modèles et spécifications

FortiGate NGFW est disponible dans de nombreux modèles différents pour répondre à vos besoins allant des appliances matérielles d'entrée de gamme aux appliances ultra haut de gamme pour répondre aux exigences de performances de protection contre les menaces les

plus exigeantes. Cela garantit que le campus d'entreprise, le centre de données central ou les segments internes, FortiGate peut s'intégrer parfaitement à votre environnement [29].

Firewall	Caractéristique
FortiGate 80F	La série FortiGate FortiWiFi 80F fournit une solution SDWAN centrée sur les applications, évolutive et sécurisée dans un format de bureau compact, sans ventilateur pour les succursales d'entreprise et les entreprises de taille moyenne avec WiFi-6 intégré (802.11ax). Protège contre les cyber menaces avec une accélération système sur puce et un SD-WAN sécurisé à la pointe de l'industrie dans une solution simple, abordable et facile à utiliser déployer la solution. L'approche Security-Driven Networking de Fortinet offre une intégration étroite du réseau à la nouvelle génération de sécurité
FortiGate 70F	La série FortiGate 70F fournit une solution SD-WAN rapide et sécurisée dans un boîtier compact sans ventilateur facteur de forme de bureau pour les succursales d'entreprise et les entreprises de taille moyenne. Protège contre cyber menaces avec accélération du système sur puce et SD-WAN sécurisé à la pointe de l'industrie dans un solution simple, abordable et facile à déployer. L'approche réseau basée sur la sécurité de Fortinet offre une intégration étroite du réseau à la nouvelle génération de sécurité.
FortiGate 60F	La série FortiGate/FortiWiFi 60F fournit une solution SD-WAN rapide et sécurisée dans un format compact Facteur de forme de bureau sans ventilateur pour les succursales d'entreprise et les entreprises de taille moyenne. Protège contre les cybers menaces avec une accélération système sur puce et un SDWAN sécurisé à la pointe de l'industrie dans une solution simple, abordable et facile à déployer. La mise en réseau axée sur la sécurité de Fortinet offre une intégration étroite du réseau à la nouvelle génération de sécurité.
FortiGate 60F - Rugged	Alors que les solutions de sécurité traditionnelles sont conçues et destinées pour le monde des bureaux et des entreprises, le FortiGate. La série Rugged offre un tout-en-un renforcé industriellement dispositif de sécurité offrant une protection spécialisée contre les menaces pour sécuriser les réseaux critiques industriels et de contrôle contre attaques malveillantes.
FortiGate 60E	Le FortiGate 60E-POE fournit une solution SD-WAN centrée sur les applications, évolutive et sécurisée dans un facteur de forme de bureau compact sans ventilateur pour les succursales d'entreprise et les entreprises de taille moyenne. Protège contre les cybermenaces grâce à l'accélération du système sur puce et à la pointe de l'industrie Sécurisez le SD-WAN dans une solution simple, abordable et facile à déployer. La sécurité de Fortinet L'approche de mise en réseau offre une intégration étroite du réseau à la nouvelle génération de Sécurité.

FortiGate 40F	La série FortiGate/FortiWiFi 40F fournit une solution SD-WAN rapide et sécurisée dans un format compact Facteur de forme de bureau sans ventilateur pour les succursales d'entreprise et les entreprises de taille moyenne. Protège contre les cybers menaces avec une accélération système sur puce et un SDWAN sécurisé à la pointe de l'industrie dans une solution simple, abordable et facile à déployer. La mise en réseau axée sur la sécurité de Fortinet offre une intégration étroite du réseau à la nouvelle génération de sécurité.

2.6 Pourquoi nous avons choisis Fortinet ?

Fortinet permet à ses clients de bénéficier d'une protection intelligente et transparente sur une surface d'attaque en expansion et de la puissance nécessaire pour répondre aux exigences de performance toujours plus élevées des réseaux sans frontières, aujourd'hui et demain.

2.7 Conclusion

Nous avons abordé dans ce chapitre une présentation de la Fortinet.

D'où on a commencé par une présentation de manière générale la Fortinet, et un historique de la Fortinet, la manière de pare-feu Fortinet fait protéger les données, les modèles et spécifications de chaque pare-feu. Et la fin, la cause de notre choix d'utiliser la Fortinet.

Dans le chapitre qui suit nous allons expliquer l'aspect pratique de notre travail sur logiciel Cisco Packet Tracer.

Chapitre 03 :

Environnement Simulation

3.1 Introduction

Dans cette chapitre on applique notre travail demande sur logiciel Cisco Packet Tracer. D'abord on commence par la présentation de logiciel Cisco Packet Traceret par la suite la configuration de notre schéma.

3.2 Présentation et utilisation de Cisco Packet Tracer

Paquet Tracer est un logiciel de CISCO permettant de construire un réseau physique virtuel et de simuler le comportement des protocoles réseaux sur ce réseau. L'utilisateur construit son réseau à l'aide d'équipements tels que les routeurs, les commutateurs ou des ordinateurs. Ces équipements doivent ensuite être reliés via des connexions (câbles divers, fibre optique). Une fois l'ensemble des équipements reliés, il est possible pour chacun d'entre eux, de configurer les adresses IP, les services disponibles, etc. . . . [14]

3.2.1 Description générale

La figure 22 montre un aperçu général de Paquet Tracer. La zone (1) est la partie dans laquelle le réseau est construit. Les équipements sont regroupés en catégories accessibles dans la zone (2). Une fois la catégorie sélectionnée, le type d'équipement peut être sélectionné dans la zone (3). La zone (6) contient un ensemble d'outils :

– Select : pour déplacer ou éditer des équipements.

– Move Lay-out : permet de déplacer le plan de travail.

– Place Note : place des notes sur le réseau.

– Délaite : supprime un équipement ou une note.

– Inspecte : permet d'ouvrir une fenêtre d'inspection sur un équipement (table ARP, routage).

La zone (5) permet d'ajouter des indications dans le réseau. Enfin, la zone (4) permet de **passer du mode temps réel au mode simulation [14].**

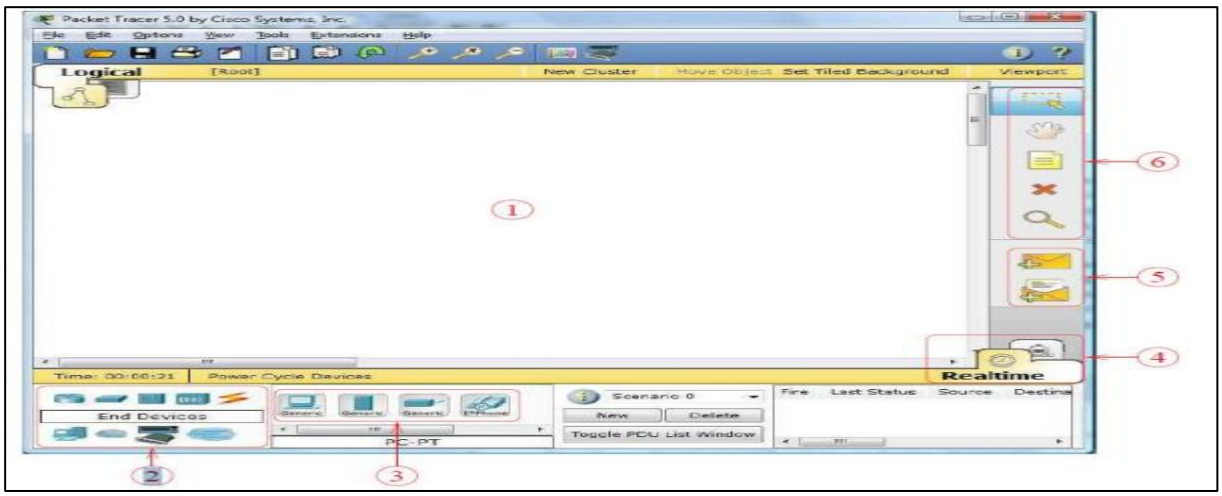

Figure 15 : interface de Paquet Tracer.

3.2.2 Construire un réseau

Pour construire un réseau, l'utilisateur doit choisir parmi les 8 catégories proposées par Paquet Tracer : les routeurs, les switches, les hubs, les équipements sans-fil, les connexions, les équipements dits terminaux (ordinateurs, serveurs), des équipements personnalisés et enfin, une connexion multi-utilisateur. Lorsqu'une catégorie est sélectionnée, l'utilisateur a alors le choix entre plusieurs équipements différents. Pour ajouter un équipement, il suffit de cliquer dessus puis de cliquer à l'endroit choisi. La figure 23 correspond à la zone décrite [14].

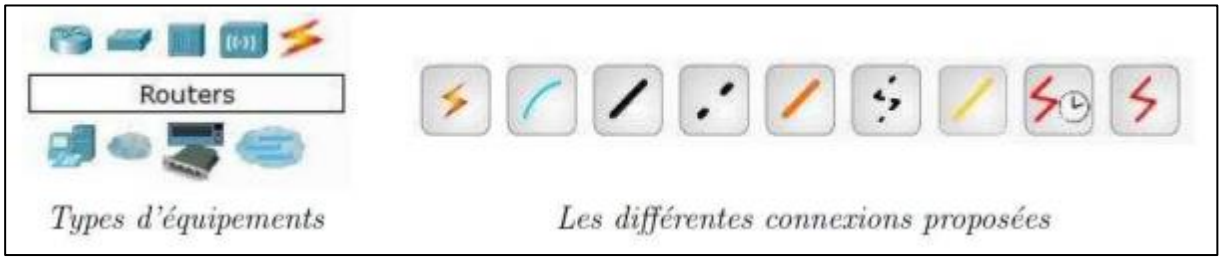

Figure 16 : la zone décrite.

Pour relier deux équipements, il faut choisir la catégorie "Connections" puis cliquer sur la connexion désirée. Dans nos différents travaux pratiques, nous n'utiliserons que 2 sortes de connexions : les câbles droits et les câbles croisés. Ils sont en position 3 et 4 sur la partie droite de la figure 23 [14].

3.2.3 Configuration d'un équipement

Lorsqu'un ordinateur a été ajouté (appelé PC-PT dans Paquet Tracer), il est possible de le configurer en cliquant dessus, une fois ajouté dans le réseau. Une nouvelle fenêtre s'ouvre comportant 3 onglets : Physical (aperçu réel de la machine et de ses modules), Config (configuration passerelle, DNS et adresse IP) et Desktop (ligne de commande ou navigateur Web). Dans l'onglet Config, il est possible de configurer la passerelle par défaut, ainsi que l'adresse du serveur DNS (cliquez pour cela sur le bouton Settings en-dessous du bouton Global). Il est possible aussi de configurer l'adresse IP et le masque de sous-réseau (cliquez pour cela sur le bouton Fast Ethernet en dessous du bouton INTERFACE), Voir figure 24 [14].

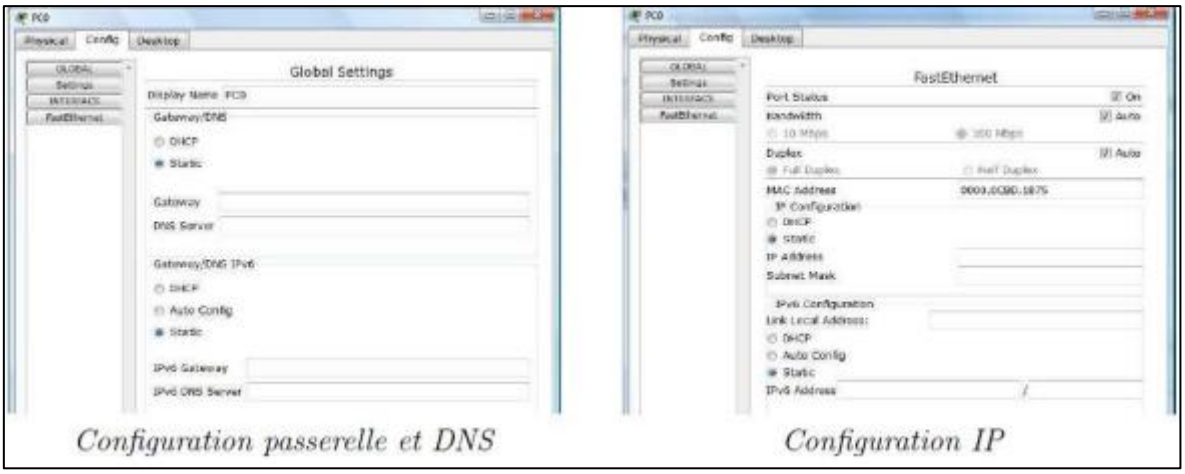

Figure 17 : configuration de PC.

3.2.4 Mode simulation

Une fois le réseau créé et prêt à fonctionner, il est possible de passer en mode simulation, ce qui permet de visualiser tous les messages échangés dans le réseau. En mode simulation, la fenêtre principale est scindée en deux, la partie de droite permettant de gérer le mode simulation : exécution pas-à-pas, vitesse de simulation, protocoles visibles. La partie gauche de la figure 25 montre la partie simulation et sa partie droite montre les détails obtenus en cliquant sur un message (ici HTTP) [14].

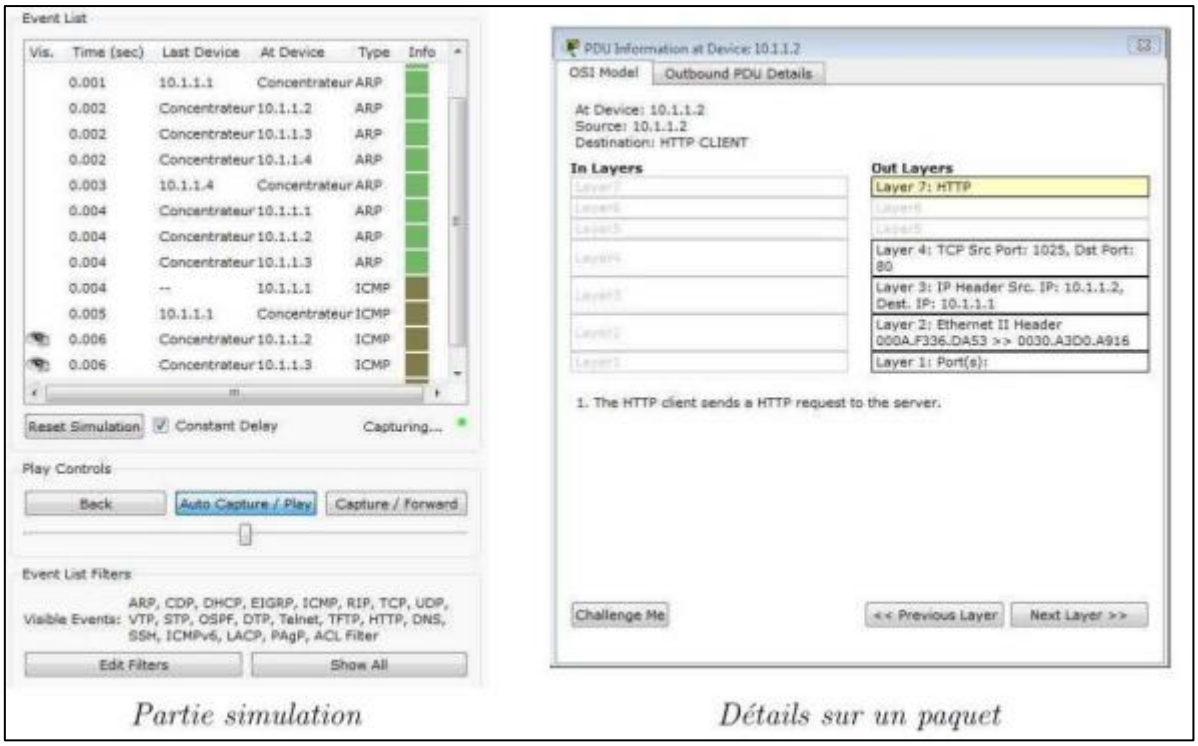

Figure 18 : la partie simulation et les détails obtenus.

3.2.5 Invite de commandes

Il est possible d'ouvrir une invite de commandes sur chaque ordinateur du réseau. Elle est accessible depuis le troisième onglet, appelé Desktop, accessible lorsque l'on clique sur un

ordinateur pour le configurer (mode sélection). Cet onglet contient un ensemble d'outils dont l'invite de commandes (Command prompt) et un navigateur Internet (Web Browser). L'invite de commandes permet d'exécuter un ensemble de commandes relatives au réseau. La liste est accessible en tapant help. En particulier, les commandes ping, ARP, traceret et ipconfig sont accessibles. Si Paquet Tracer est en mode simulation, les messages échangés suite à un appel à la commande ping peuvent ainsi être visualisés [14].

3.3 Configuration de sécurité d'un réseau sur paquet tracer

L'ASA (Adaptive Security Appliance) est un produit de sécurité réseau qui fait partie du portefeuille Advanced Network Firewall de Cisco. On va l'utilise sur notre réseau comme il est sur la figure 26.

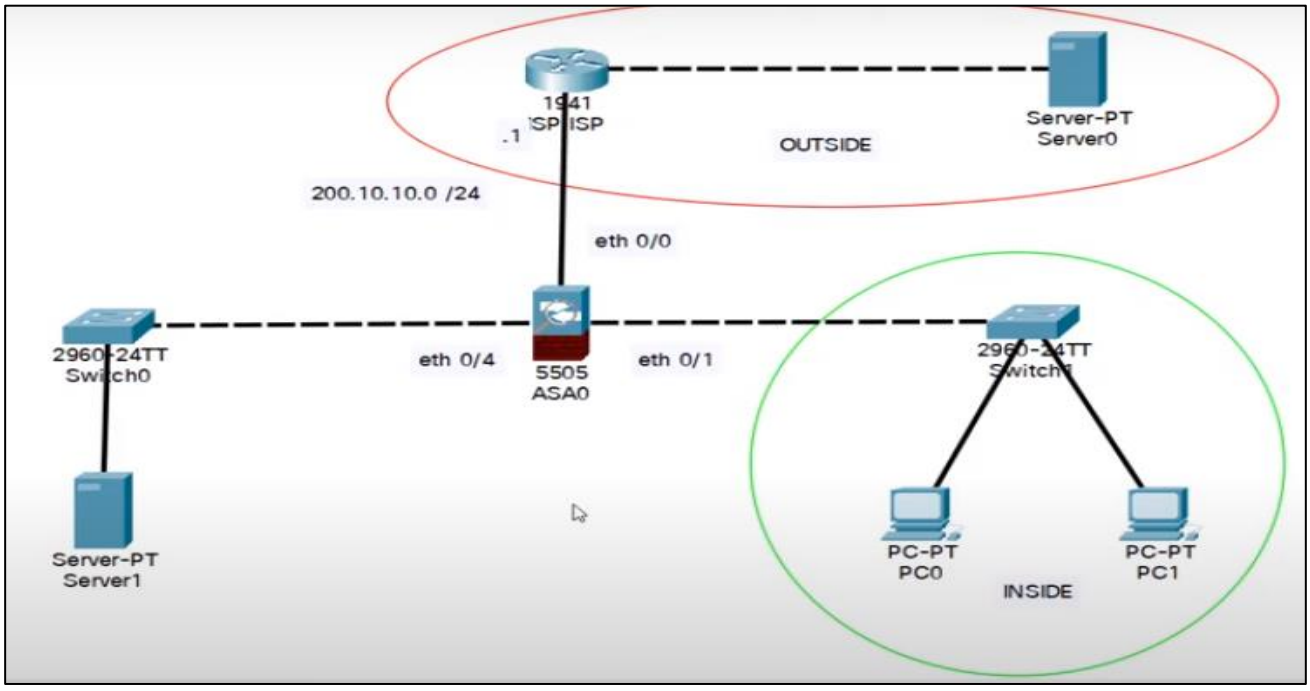

Figure 19 : firewall ASA sur notre réseau.

Notre réseau est composé à 3 parties à cause de firewall ASA la première est inside zone c'est la zone prive leur niveau de sécurité est 100, la deuxième partie outside zone partie publique internet leur niveau de securit est 0 et la troisième partie c'est DMZ pour les serveurs et tout leur niveau de securit est configurable sur le pare-feu. La règle de ASA dit que le grand niveau de securit il peu accède au niveau qu'est inferieur que lui. ASA il se compose de 8 portes le 6 et 7 sont pour Ethernet VLAN2, 0 par default outside et les autres par configuration VLAN1 sans oublie USB et console. Voir figure 27.

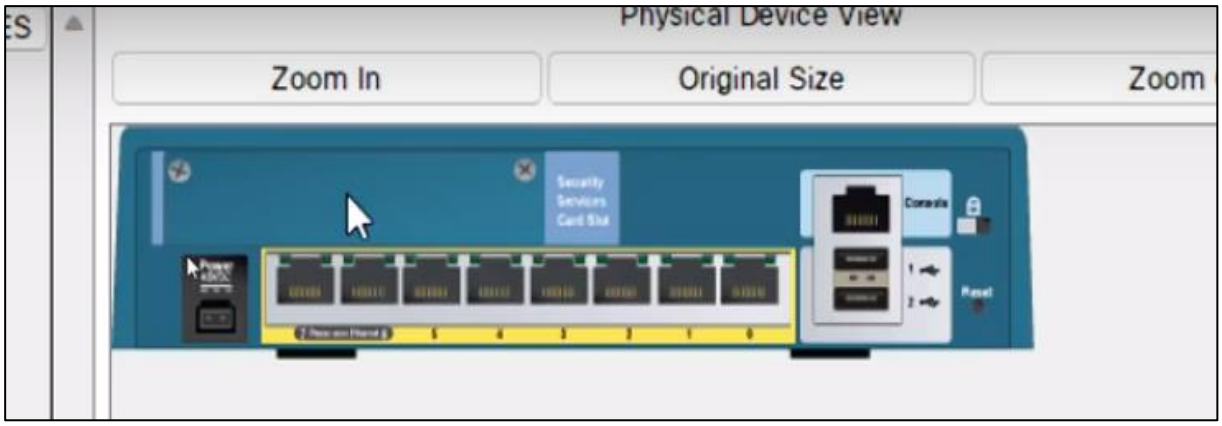

Figure 16 : les ports de CISCO ASA.

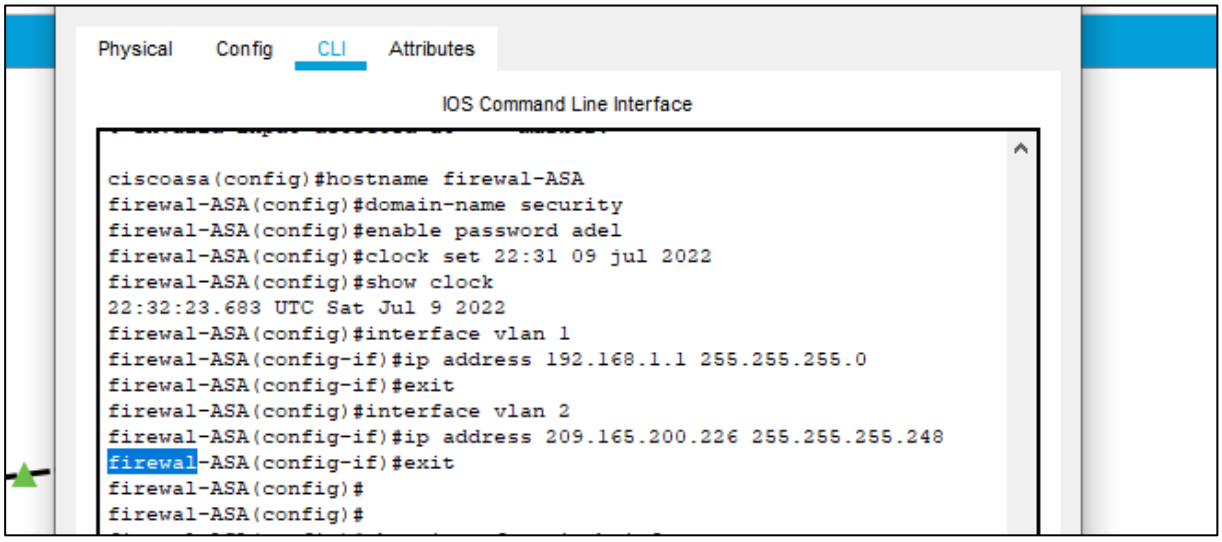

Figure 17 : authentification de firewall.

Au début on le donne un nom, leur nom de domaine, mot de passe, la date et l'heure et donne la deuxième parte on donne l'adresse IP et le masque de chaque VLAN.

Et la figure 29 on voir la vérification des adresses IP.

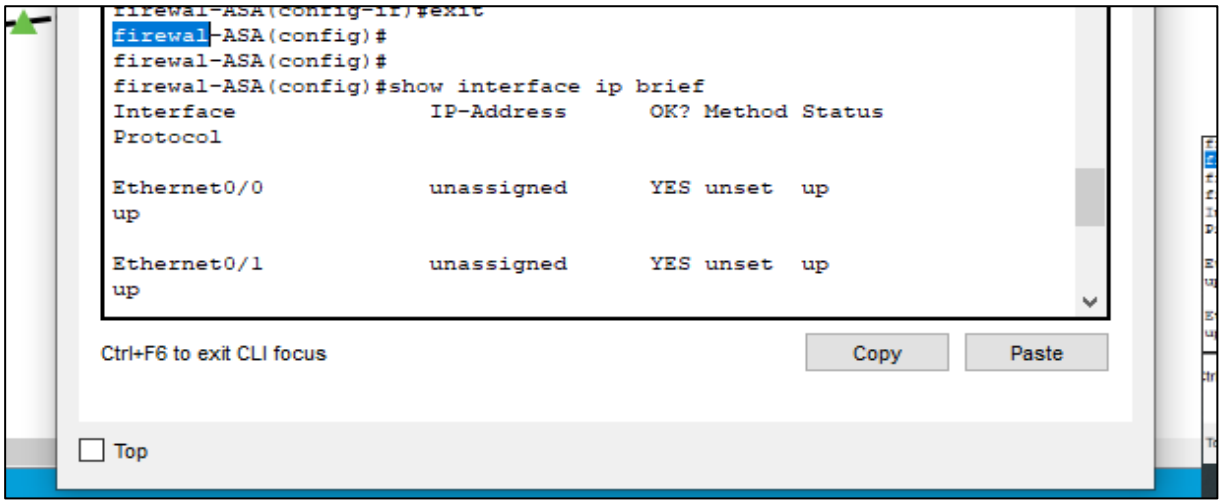

Figure 18 : vérification des adresses IP.

3.4 Configuration de routeur

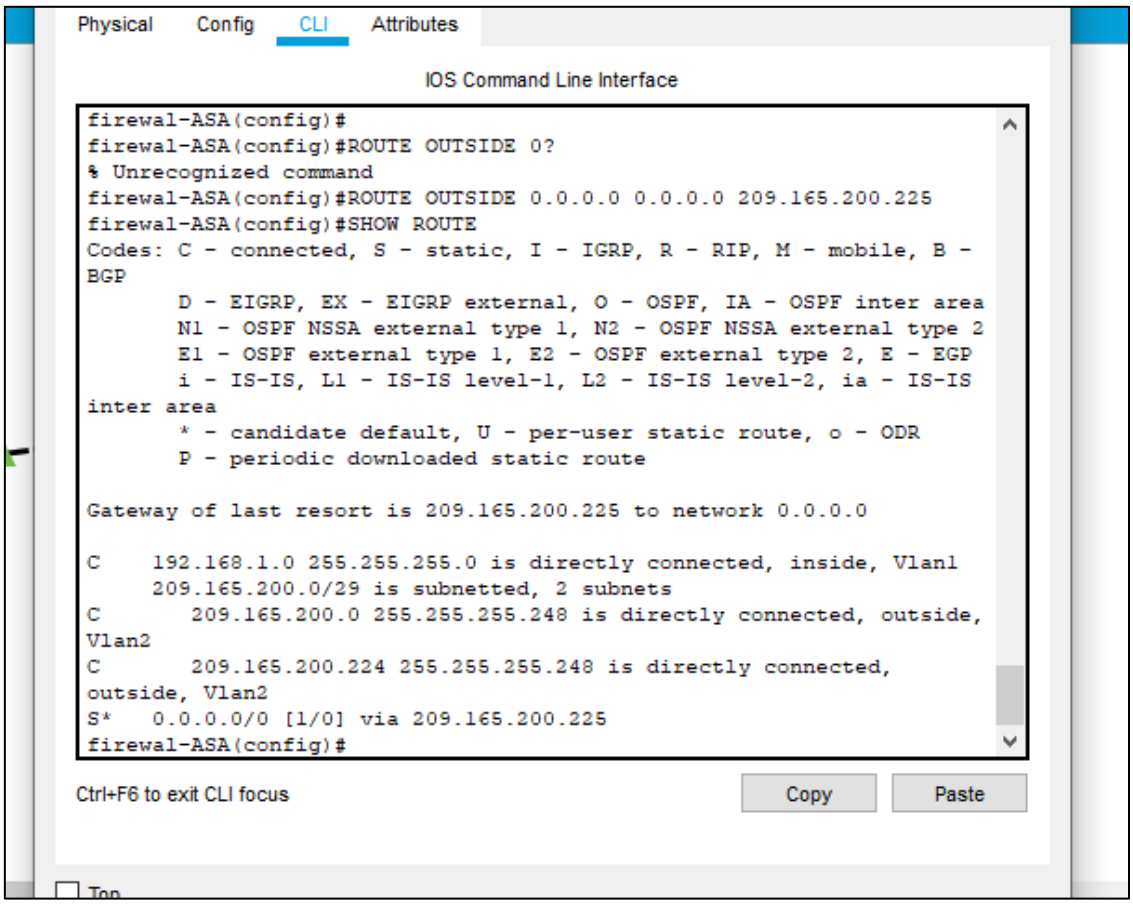

Figure 19 : configuration de routeur.

Dans la configuration du retour ont utilisé la commande route et on précise la sortie OUTSIDE et on donne l'adresse de prochain hub, ensuite on confirme de notre configuration.

3.5 Configuration du serveur

Le protocole DHCP (Dynamic Host Configuration Protocol) est un protocole client/serveur qui fournit automatiquement un hôte IP (Internet Protocol) avec son adresse IP et d'autres informations de configuration associées, telles que le masque de sous-réseau et la passerelle par défaut [15].

3.6 Les ports et le protocole de couche 4 utilisés par DHCP

Le protocole DHCP permet la configuration dynamique de paramètres réseau en gérant une base de données de paramètres configurables pour chacun des ordinateurs sur le réseau. DHCP permet aussi l'allocation dynamique d'adresses IP. [15]

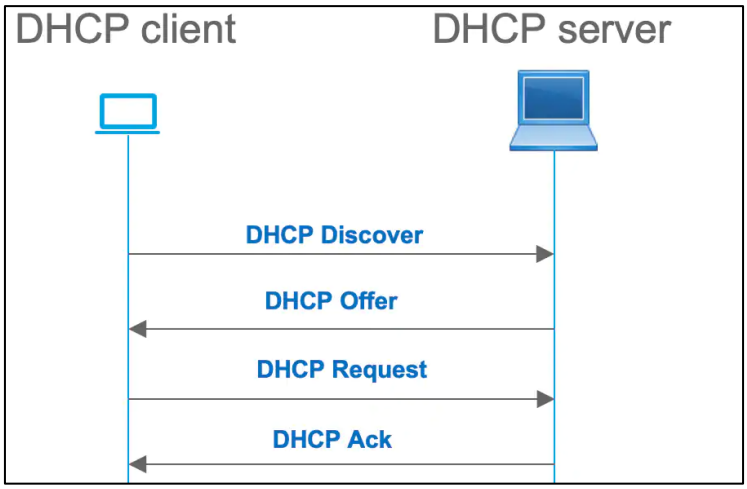

Figure 24 : les couches DHCP.

3.7 Numéro de port du service DHCP lors de l'attribution d'une adresse IP

Le port par défaut est le 67. Le serveur DHCP transmet les réponses aux clients DHCP à un numéro de port supérieur au port UDP spécifié. Par exemple, si vous acceptez le port 67 (port par défaut), le serveur attend sur le port 67 les requêtes et sur le port 68 les réponses au client [15].

3.7.1 Pourquoi DHCP utilisé UDP ?

Les messages DHCP sont transmis via UDP. Bien que peu fiable, ce protocole suffit au transport des paquets simples sur réseau local, et surtout il est très léger, donc intéressant pour les petits systèmes (du genre le micro bout de programme qui fait la requête DHCP lorsque le PC se met en route) [15].

3.7.2 Configuration de notre réseau

En configurant le service DHCP sur votre réseau, vous configurez et démarrez le premier serveur DHCP. Vous pourrez par la suite ajouter d'autres serveurs DHCP en leur donnant accès aux mêmes données depuis un emplacement partagé, à condition que le magasin de données gère les données partagées [15].

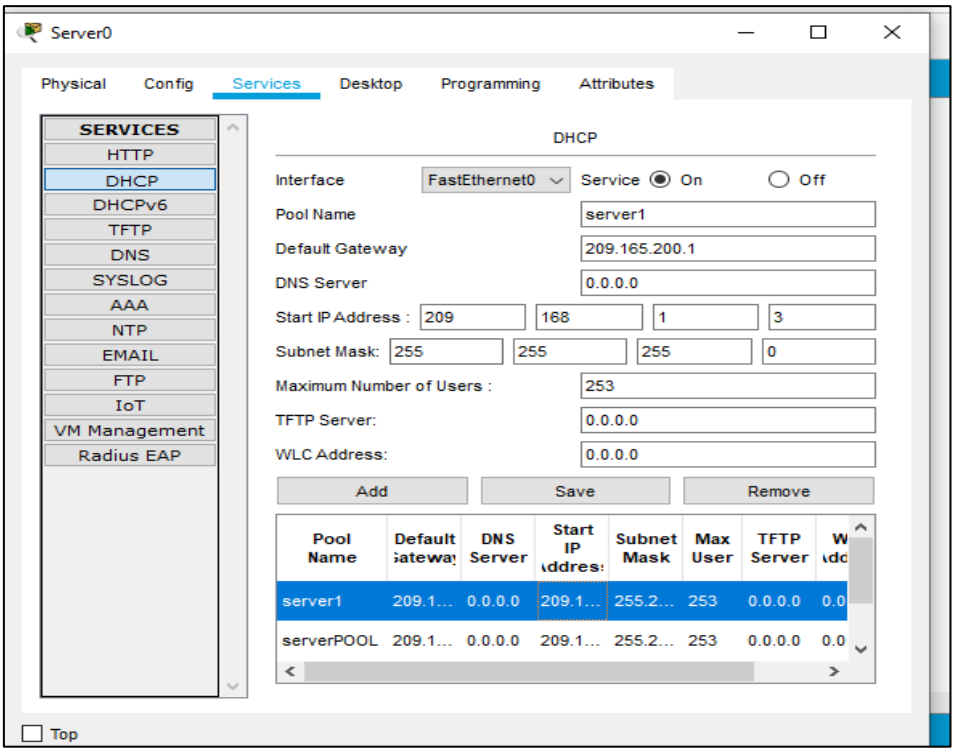

Figure 25 : configuration de serveur DHCP.

On a créé deux serveurs en donnant GETEWAY par default et adresse IP de démarrage et en active serveur après l'enregistrement.

3.8 Configuration des adresses IP

Tout le pc prenant des adresses à partir de serveur DHCP.

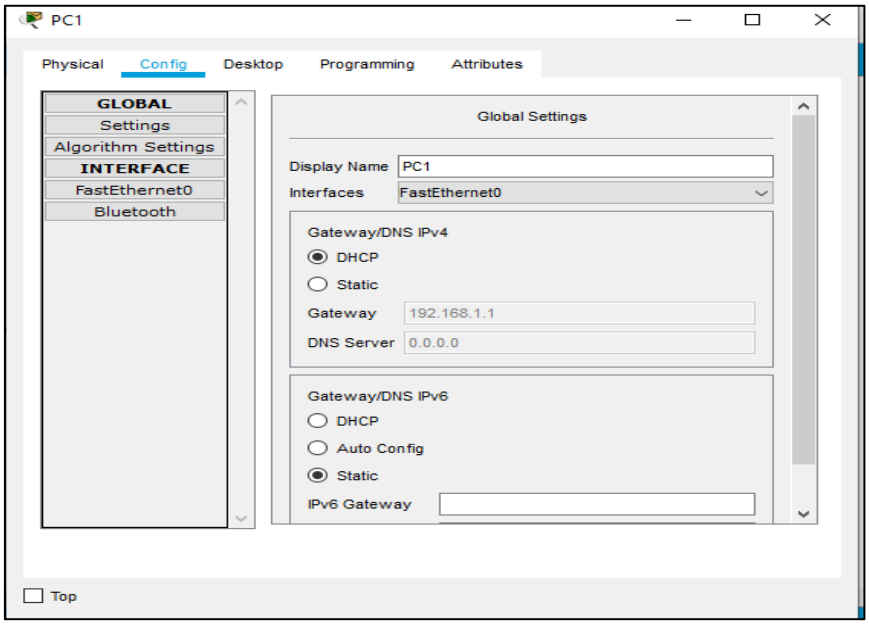

Figure 20 : Activation l'adressage automatique sur le PC.

3.9 La traduction d'adresses de port (PAT)

Est une fonction qui permet à plusieurs utilisateurs au sein d'un réseau privé d'utiliser un nombre minimal d'adresses IP. Sa fonction de base est de partager une seule adresse IP publique entre plusieurs clients qui ont besoin d'utiliser Internet publiquement. Il s'agit d'une extension de la traduction d'adresses réseau (NAT).La traduction d'adresse de port est également connue sous le nom de surcharge ou de surcharge de port[16].

3.9.1 La défiance entre NAT et PAT

La surcharge NAT ou la traduction d'adresses de port (PAT) est une forme modifiée de NAT dynamique où le nombre d'adresses locales internes est supérieur au nombre d'adresses globales internes. La plupart du temps, il n'y a qu'une seule adresse IP globale interne fournissant un accès Internet à tous les hôtes internes [16].

3.9.2 Le fonctionnement de PAT CISCO

Il fonctionne en créant un mappage NAT dynamique, dans lequel une adresse IP globale (publique) et un numéro de port unique sont sélectionnés. Le routeur conserve une entrée de table NAT pour chaque combinaison unique de l'adresse IP privée et du port, avec une traduction à l'adresse globale et un numéro de port unique [16].

3.10 Politique d'inspection pare feu

L'inspection avec état, également appelée filtrage dynamique des paquets, est une technologie de pare-feu qui surveille l'état des connexions actives et utilise ces informations pour déterminer les paquets réseau à autoriser à traverser le pare-feu.

3.11 AAA authentification

L'authentification est la première étape du processus de sécurité AAA et décrit la façon dont le réseau ou les applications permettent d'identifier un utilisateur et de s'assurer que l'utilisateur est bien celui qu'il prétend être. L'utilisateur entre un nom d'utilisateur et un mot de passe valides avant d'y accéder, chaque utilisateur doit disposer d'un ensemble unique d'informations d'identification.

3.12 Configuration de DMZ

La partie DMZ on la crée pour publie les sites, les emails et tous les choses publiques.

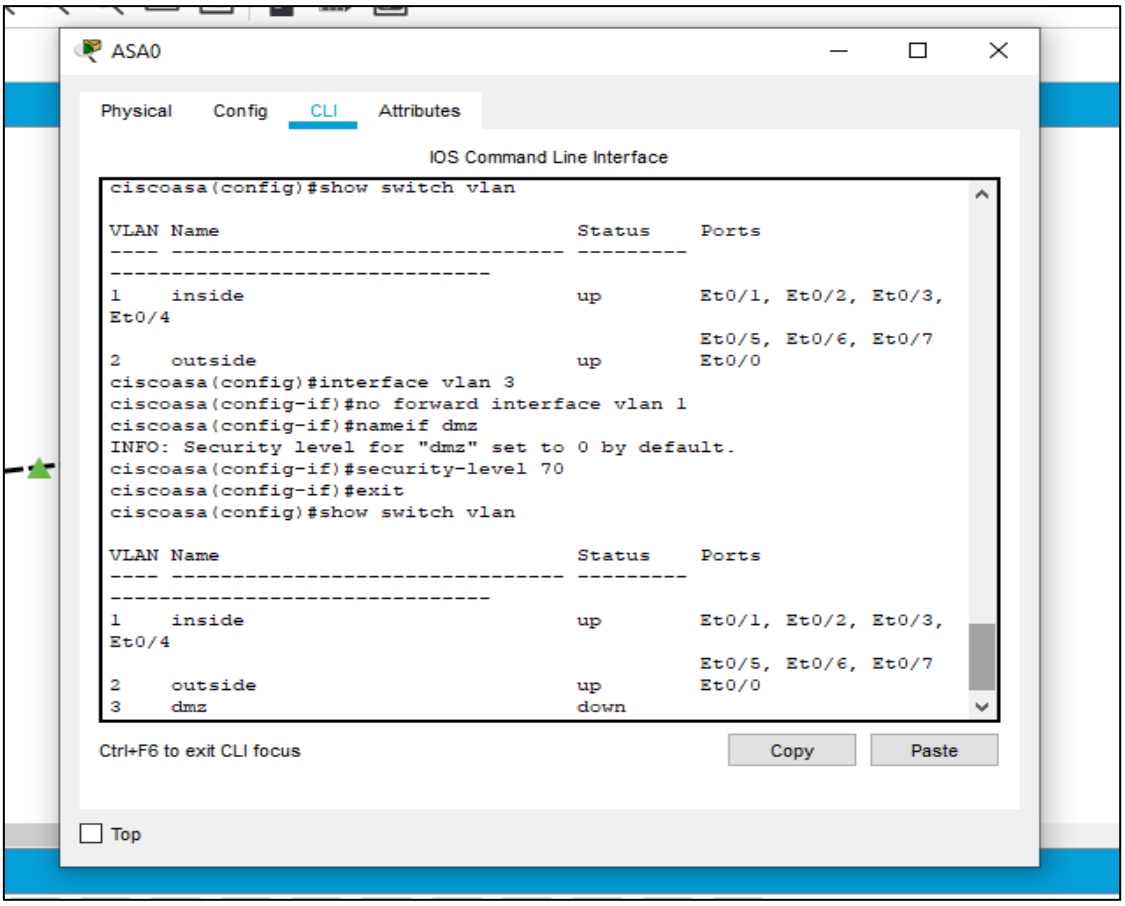

Figure 27 : L'autorisation de la zone DMZ.

Au début on a vu les VLANS qui sont au notre pare-feu ils sont deux, on suite on a créé VLAN 3 et l'interdit d'accède à VLAN 1, j'ai la donne le nom DMZ a cette zone et change le niveau de securit de 0 par default a 70.

Dans ce cas le niveau de securit est 70 pour autorise les utilisateurs de outside accède à cette zone il faut utilisée les ACL comme il est à la figure 28.

Maintenant notre problème est VLAN 3 est down parce qu'elle a plus de porte, il faut la donne une porte et ça avec Access liste.

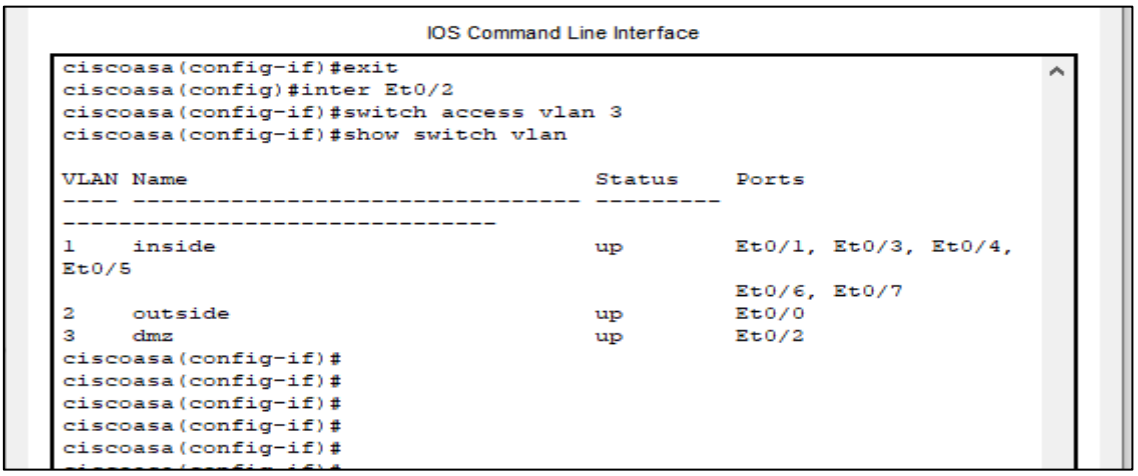

Figure 28 : configuration de l'Access liste vlan 3.

On a accédé à l'interface ETH 0/2 on donne l'accès à cette zone par cette interface après on confirme qu'elle est up**.**

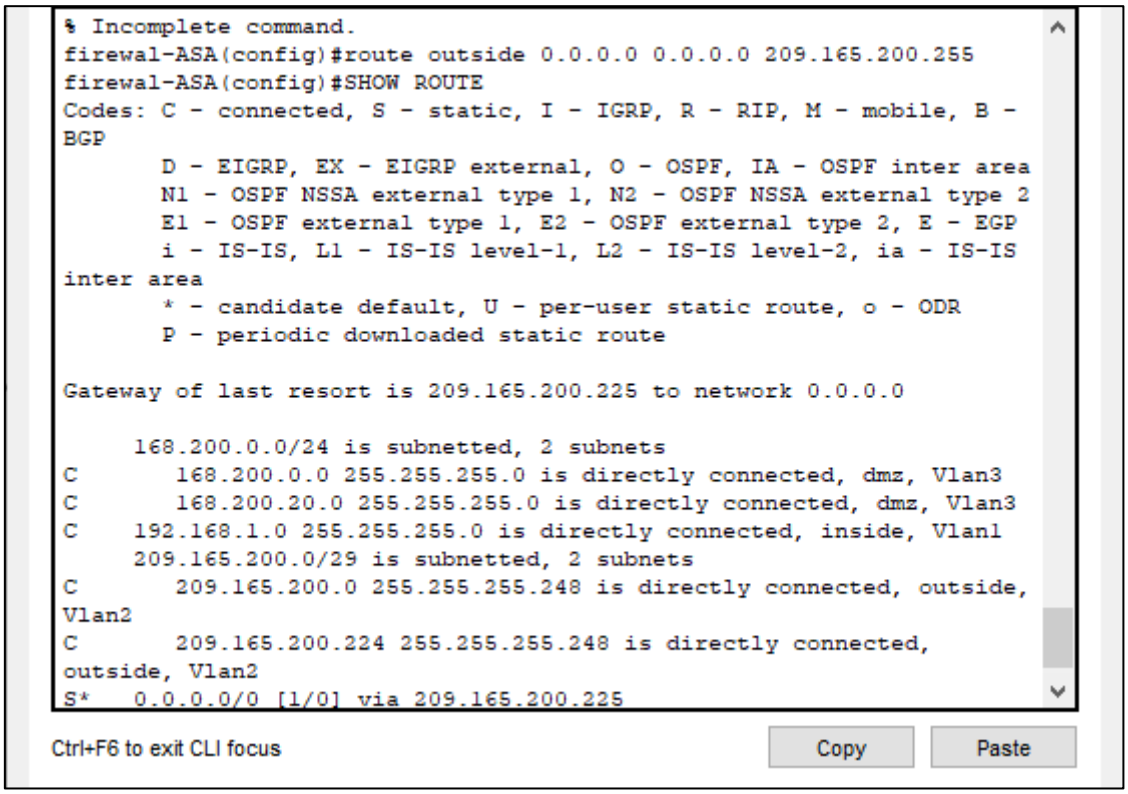

Figure 29 : configuration le control de la sortie.

```
firewal-ASA(config-network-object)#NAT (INSIDE,OUTSIDE) DYNAMIC
INTERFACE
firewal-ASA(config-network-object)#
```

Figure 30 : configuration service NAT sur le firewall.

3.13 Topologie de notre réseau

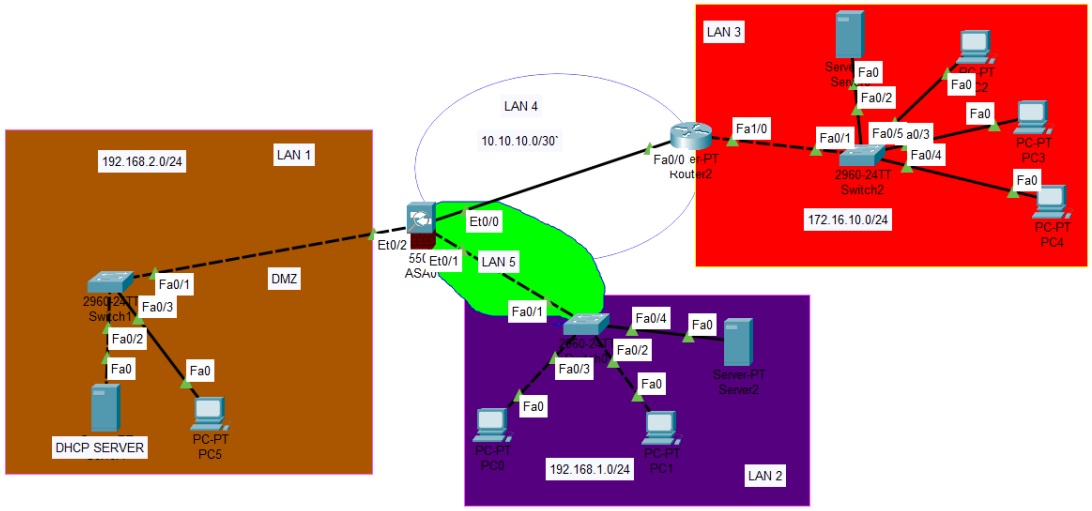

Figure 21 : Topologie de notre réseau de la société.

3.14 Conclusion :

Nous avons abordé dans ce chapitre aspect pratique de notre travail sur logiciel Cisco Packet Tracer.

On a commencé par la présentation le Cisco paquet tracer, la configuration de sécurité d'un réseau sur paquet tracer. La configuration de routeur, serveur, les ports, protocole de couche 4 par DHCP et les adresses IP. L'utilisation de la traduction d'adressages de port PAT et NAT, l'authentification AAA, la configuration de DMZ et la fin la topologie de réseau de la société.

Dans le chapitre qui suit nous allons pratiquer notre travail avec le matérielle informatique.

Chapitre 04 :

Installation et Test du pare-feu Fortinet

4.1 Introduction

Dans ce chapitre on applique notre travail avec le Fortinet d'où on commence une description générale sur la fonction de Fortinet, par la suite on commence d'appliquer la politique.

4.2 Description générale de fonctionnalité de la Fortinet

Ce schéma montre comment configurer un profil de sécurité de filtre Web avec un quota qui limite dynamiquement la durée pendant laquelle les utilisateurs d'un réseau interne peuvent accéder aux sites Web classés dans la catégorie "Intérêt général". Une licence active pour les services de filtrage WebFortiGuard est requise pour utiliser le filtrage Web avec des quotas [17].

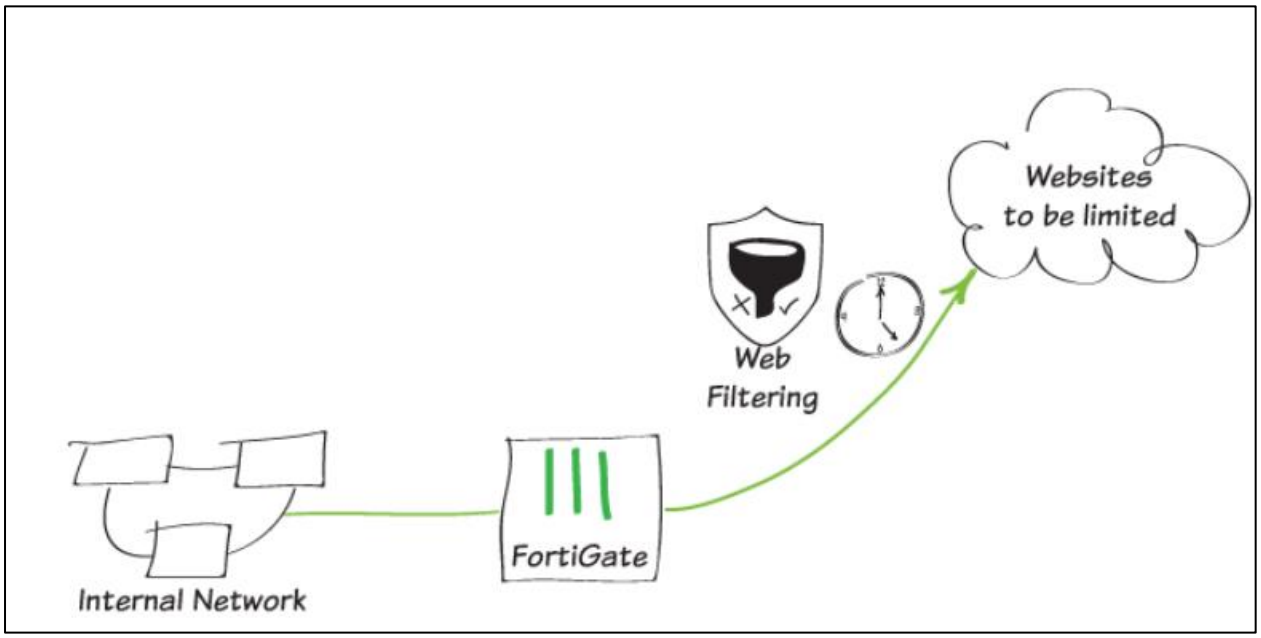

Figure 22 : Schéma descriptive pour la configuration des profils de sécurité de filtre Web avec un quota.

On peut également appliquer des quotas à des utilisateurs spécifiques sur votre réseau en créant des politiques granulaires qui appliquent différents quotas à différents groupes d'utilisateurs utilisant des adresses de pare-feu spécifiques ou nécessitant une authentification.

4.3 L'environnement de LogiTrans

Logitrans apparaîtra comme une entreprise soucieuse de l'environnement qui conçoit, fabrique et commercialise des produits de qualité.

Par conséquent, Logitrans s'engage à :

- Rester vigilante concernant son incidence interne et externe sur l'environnement
- En déployant une gestion efficace visant à prévenir la pollution et réduire les émissions de C02
- Communiquer aux parties des informations portant sur ses activités et ses résultats

- Réduire l'utilisation des ressources irremplaçables grâce à des mesures de recyclage et d'économie d'énergie
- Garantir la conformité à l'égard des textes législatifs en vigueur et des modalités relatives aux agréments environnementaux
- Suivre les évolutions en vue de satisfaire aux nouvelles demandes émanant des autorités et des clients
- Offrir un cadre de travail attrayant où l'on favorise l'engagement environnemental à travers les formations et les campagnes de sensibilisation
- Motiver nos sous-traitants et autres partenaires à un comportement éco-responsable
- Tenir compte de son impact environnemental pendant l'élaboration des nouveaux produits, réaménager la production et réaliser de nouveaux investissements [30].

4.4 L'architecture de réseau

Dans l'architecture de notre organisme d'accueille, Qui est constitue de deux server, un serveur d'accès internet et l'autre RMS qui est une liaison permanente réservée à l'usage exclusif d'un utilisateur. Elle offre la possibilité de transmission entre deux points de terminaison déterminés du réseau public. Et un Firewall Routeur qui permettre de sécurise le réseau interne, un switch et la fin les ordinateur des employées comme un PC qui a l'os kali linux et les autres l'os Windows.

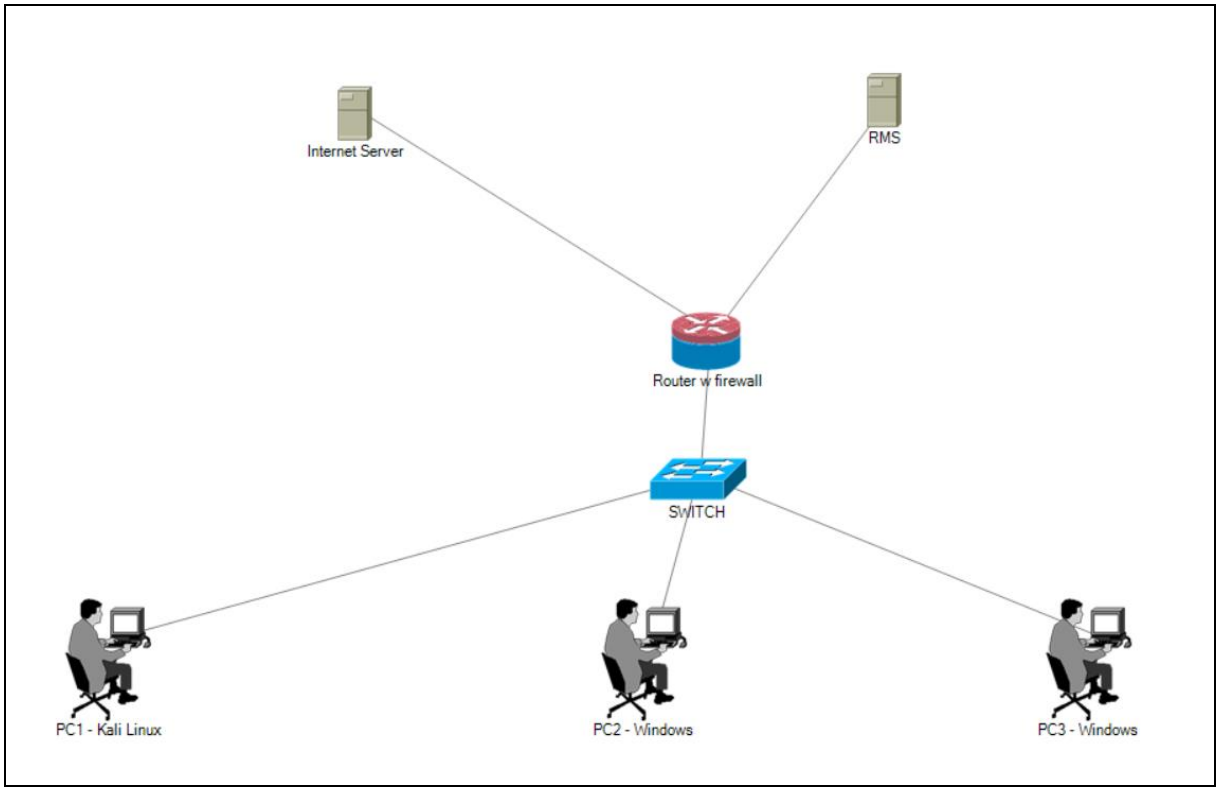

Figure 23 : l'architecture de réseau interne chez LogiTrans.

4.5 Installation du pare-feu Fortinet

Pour la démo nous avons choisie l'interface FortiGate-VM pour l'implémentation. On commence par la connections dans la plateforme.

Après la connexion, il nous affiche les informations sur les interfaces dans notre démo :

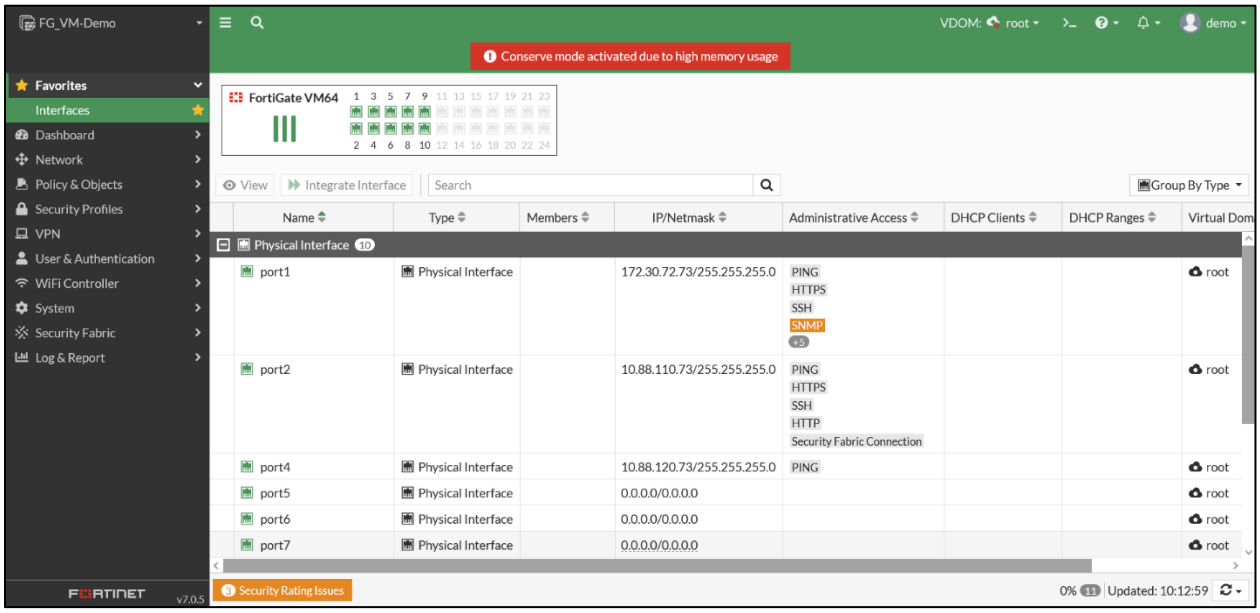

Figure 24 : Description des informations sur notre plateforme.

Dans le cas où on ne trouve pas des monitors lors de l'installation de système, on peut l'ajouter on suivant les étapes qui Suits :

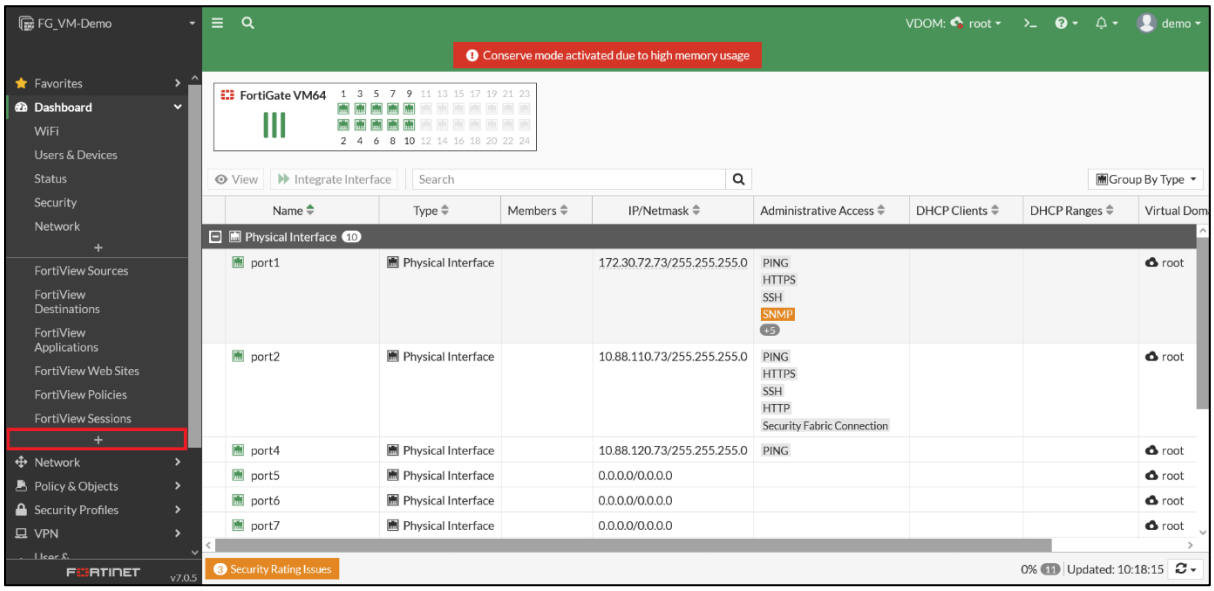

Figure 25 : Description d'un ajout d'un nouveau monitor.

Dans notre démonstration, on a pris le web filtre comme un exemple :

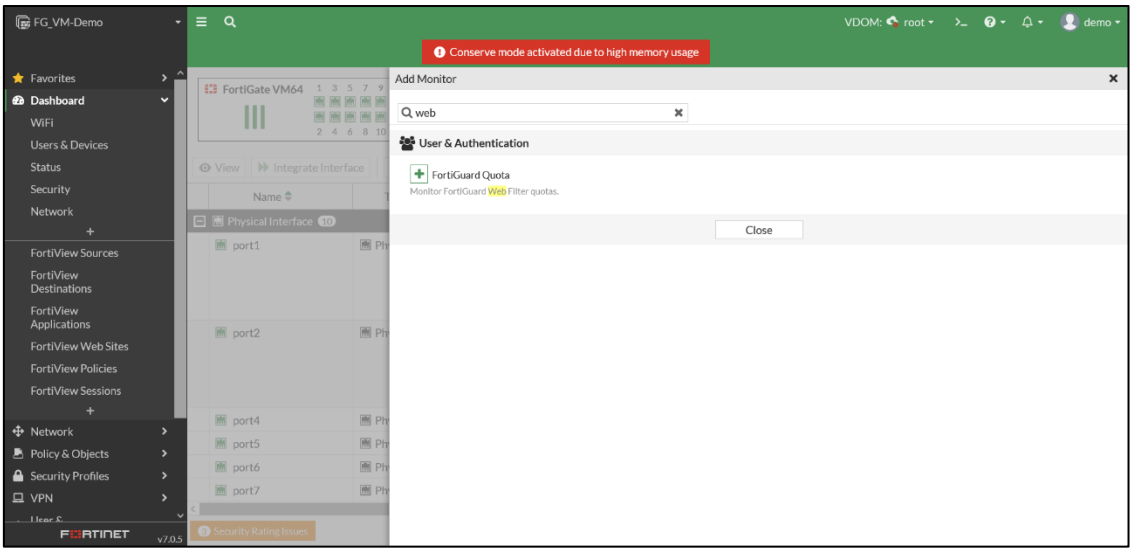

Figure 36 : Description de recherché d'un monitor.

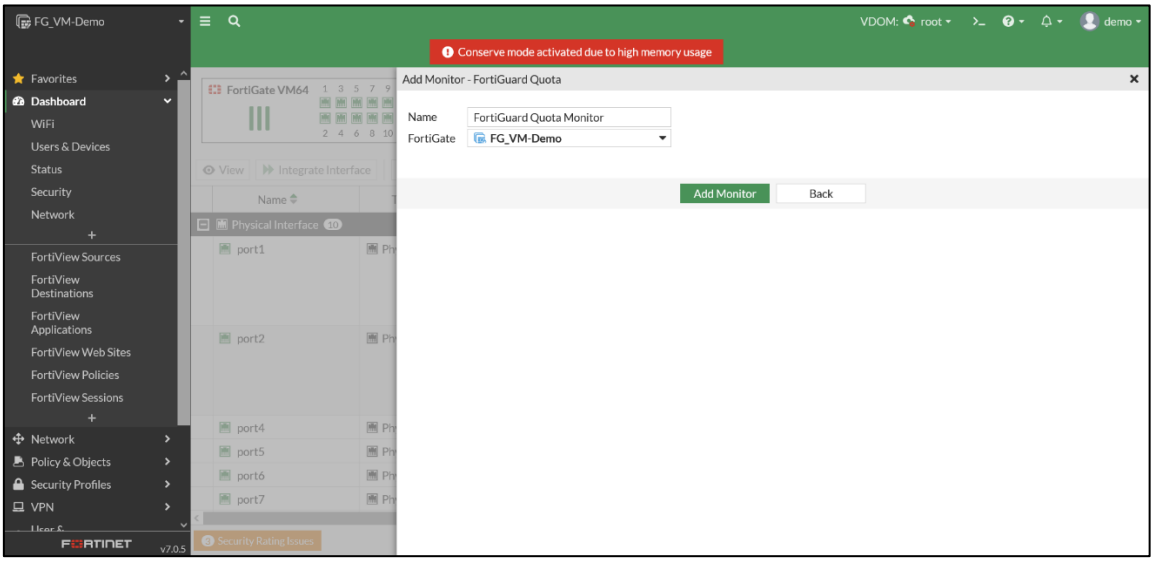

Figure 37 : Description de modification des informations sur le monitor.

Et dans notre Security & profiles, on trouve des exemples pour filtrage comme par exemple le monitor-all :

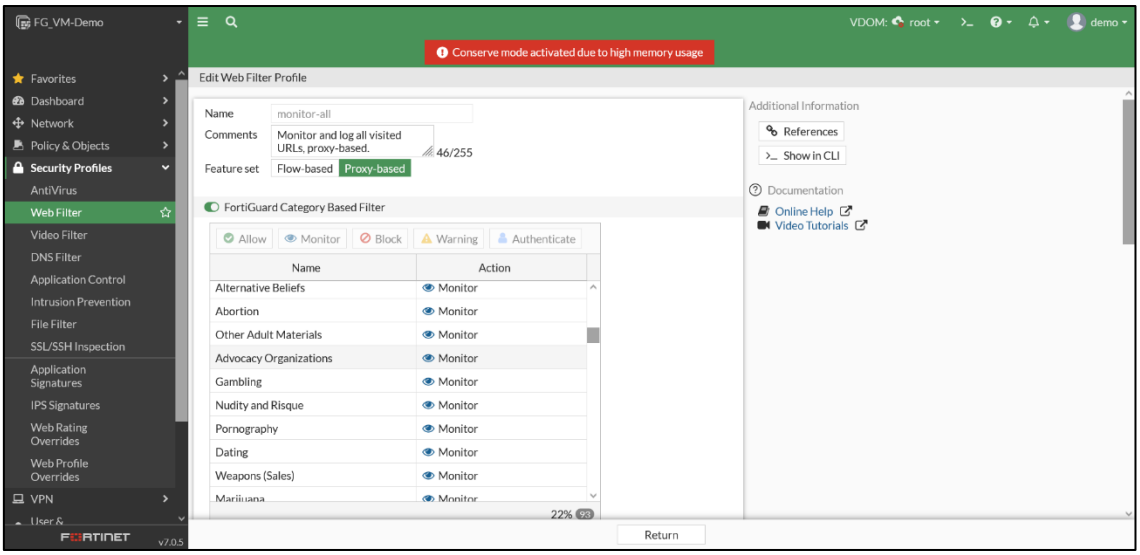

Figure 38 : Description des informations d'un filtreur de paquet.

On Remarque que notre filtre Policy est par défaut vide :

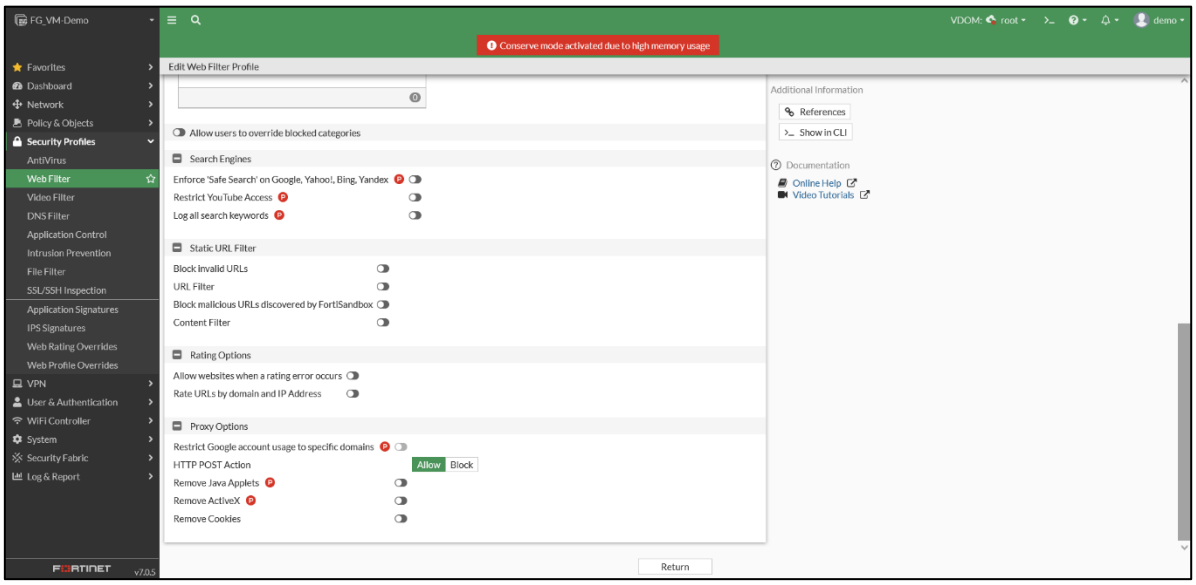

Figure 39 : Description des informations de la politique par default.

On commence par appliquer notre politique de sécurité comme par exemple :

- Filtrage les paquets de recherché sur Google engins.
- Restreinte l'Access sur YouTube.
- Enregistrer dans le journal de log tous les mots clés chercher.
- Suppression tous les ActiveX.
- La suppression des cookies.

Remarque : Le signe P veut dire que notre filtrage utilise les fonctionnalités proxy.

En appliquant la politique précédant :

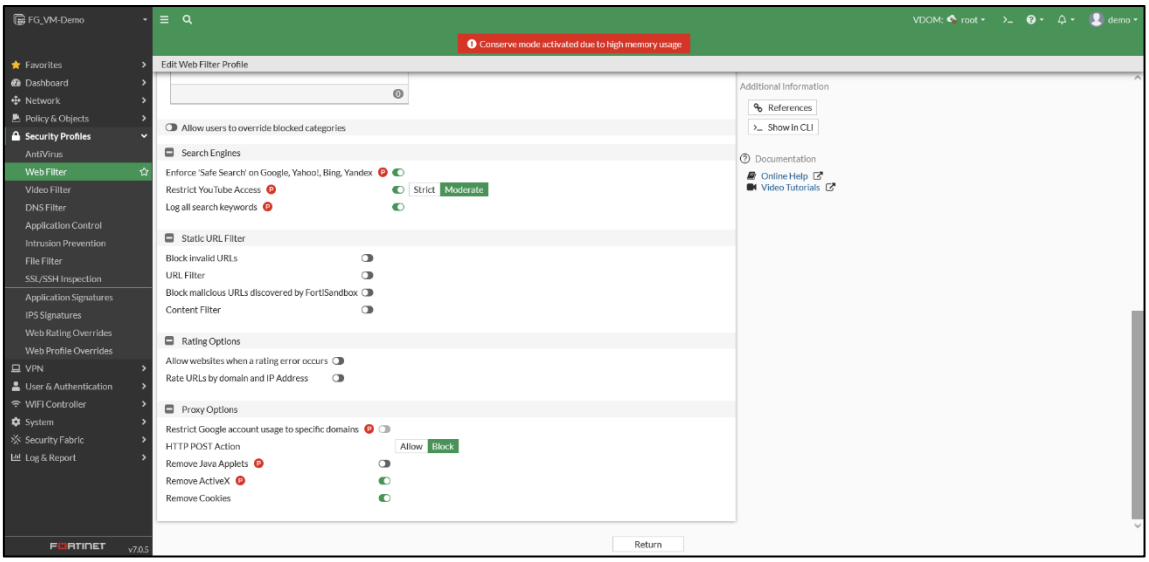

Figure 40: Application de la politique de filtrage.

4.6 Utilisation de la FortiWeb

FortiWeb déploie une approche intégrale de protection des applications web en tirant parti d'un service de réputation des IP, d'une protection contre les DDoS, d'une validation des protocoles, de signatures spécifiques aux attaques ciblant les applications, ou encore de la neutralisation des bots [18].

On commence notre analyse dans Log&Report, on commence avec le forward traffic :

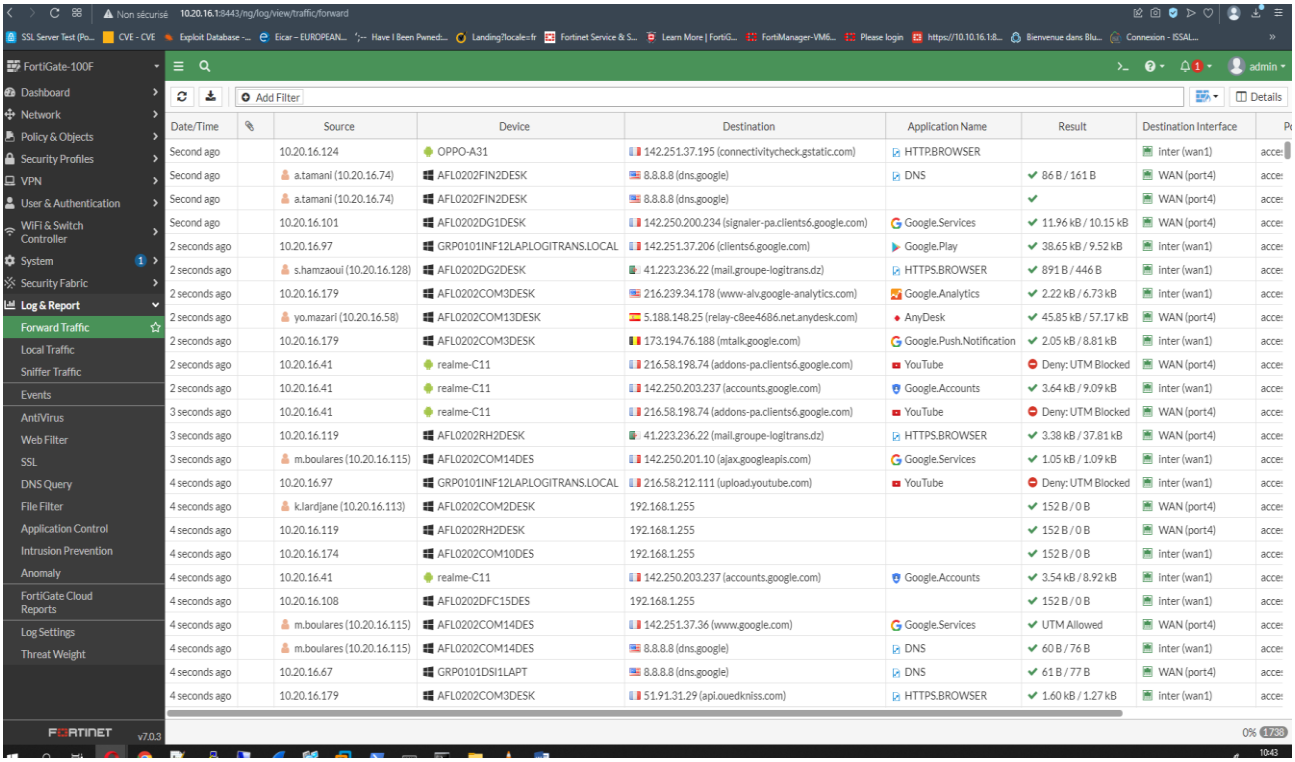

Figure 41 : Journal de capture forward traffic.

On remarque dans chaque 2 secondes, il écrit dans le journal de log tous les activités.

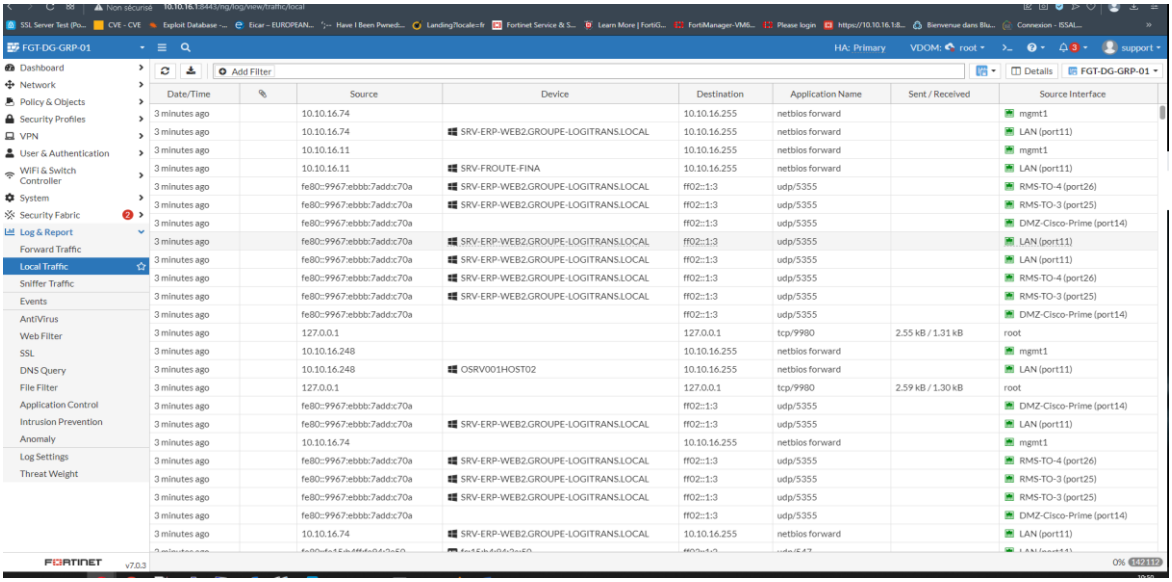

Figure 26 : Journal de capture local traffic.

On Remarque il écrit dans le journal de log tous les paquets échanges dans notre réseau locale.

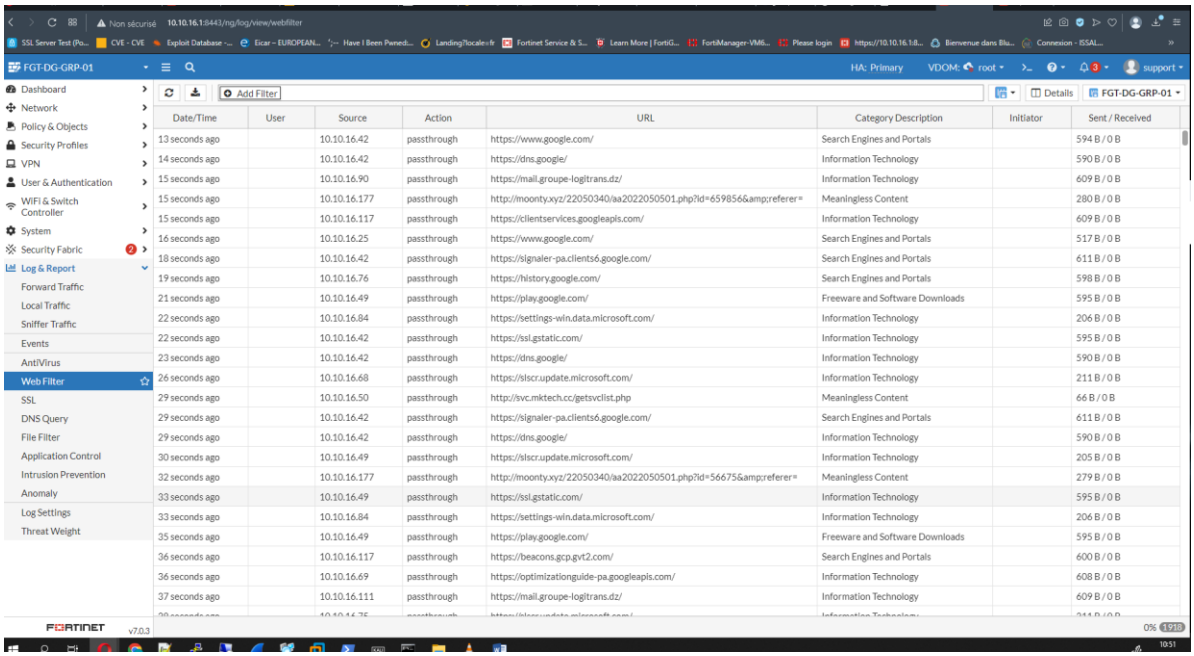

Figure 27 : Journal de capture web filter.

On Remarque il écrit dans le journal de log tous les activités dans le navigateur web de l'employé.

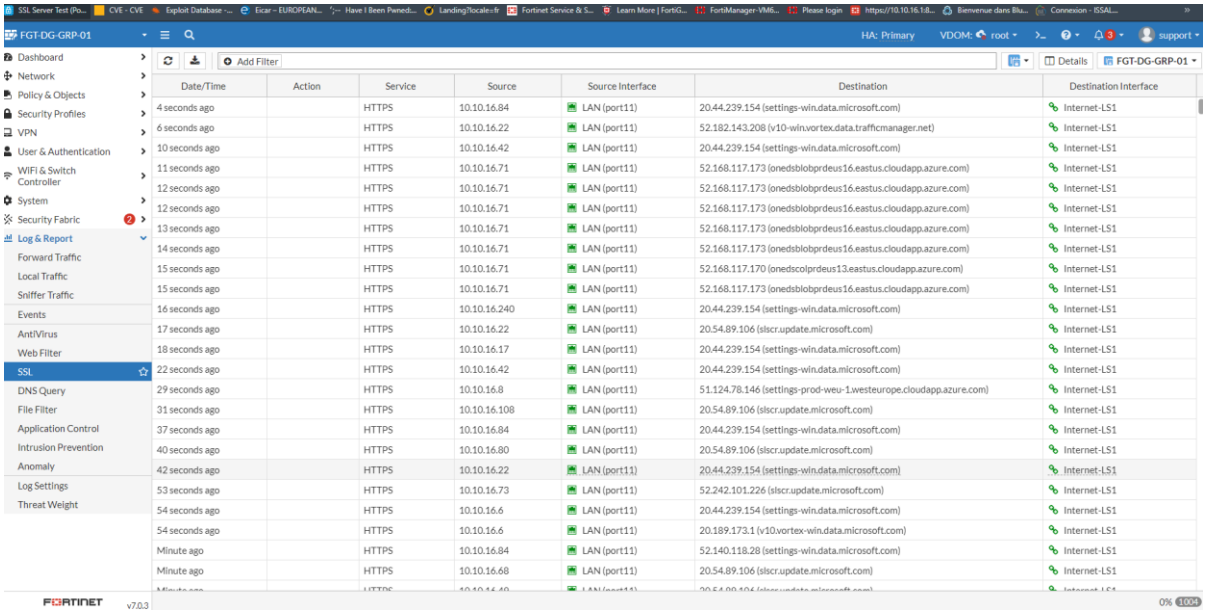

Figure 28 : Journal de capture SSL.

On Remarque il écrit dans le journal de log tous les sockets et les échanges sécurise dans le navigateur web de l'employé.

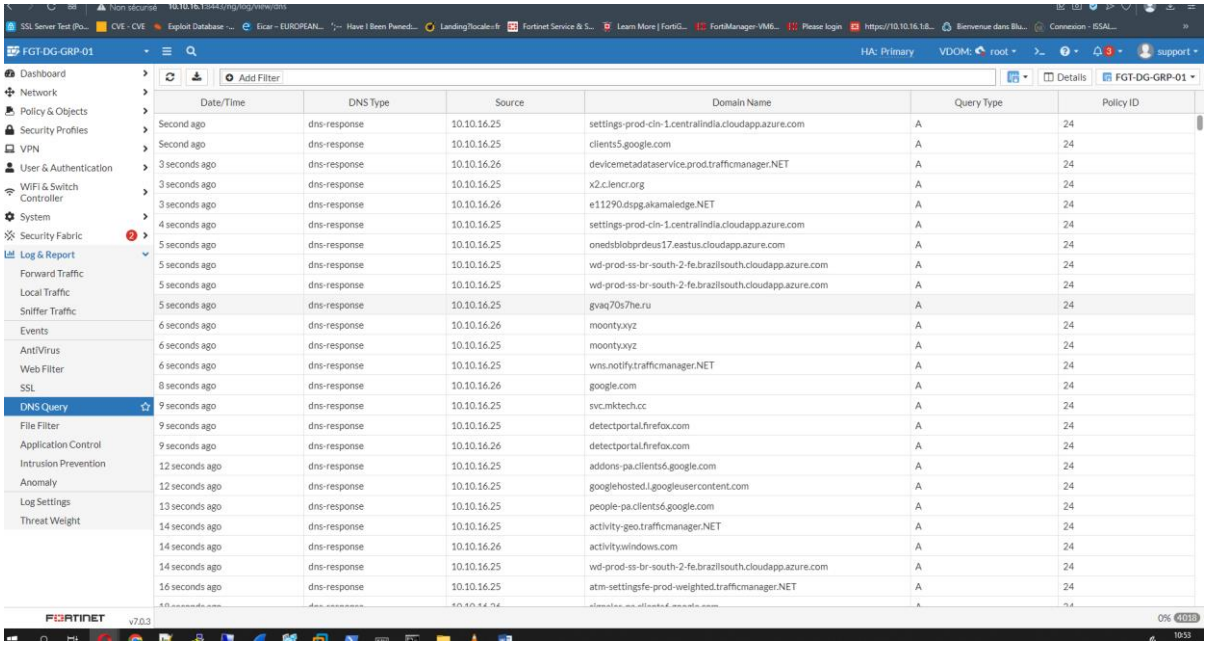

Figure 29 : Journal de capture DNS Query.

On Remarque il écrit dans le journal de log tous les échanges DNS de l'employé.

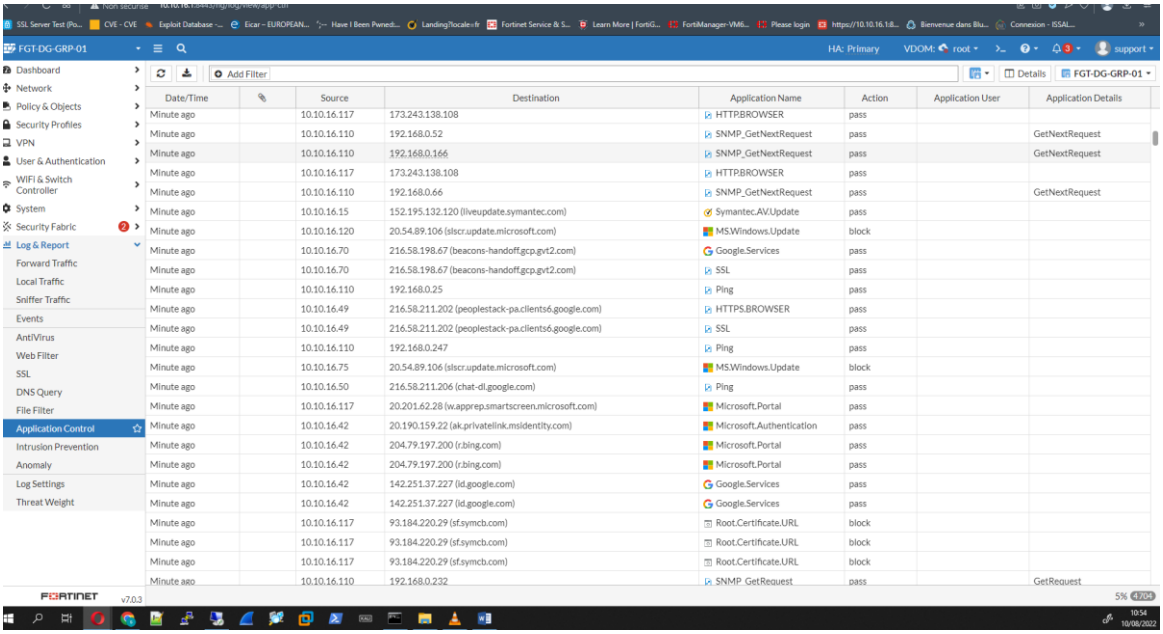

Figure 46 : Journal de filtrage l'application control.

On Remarque il écrit dans le journal de log tous les applications utiliser pour employer.

Enfin, il existe un journal pour filtrage des attaques comme par exemple les attaques DDoS.

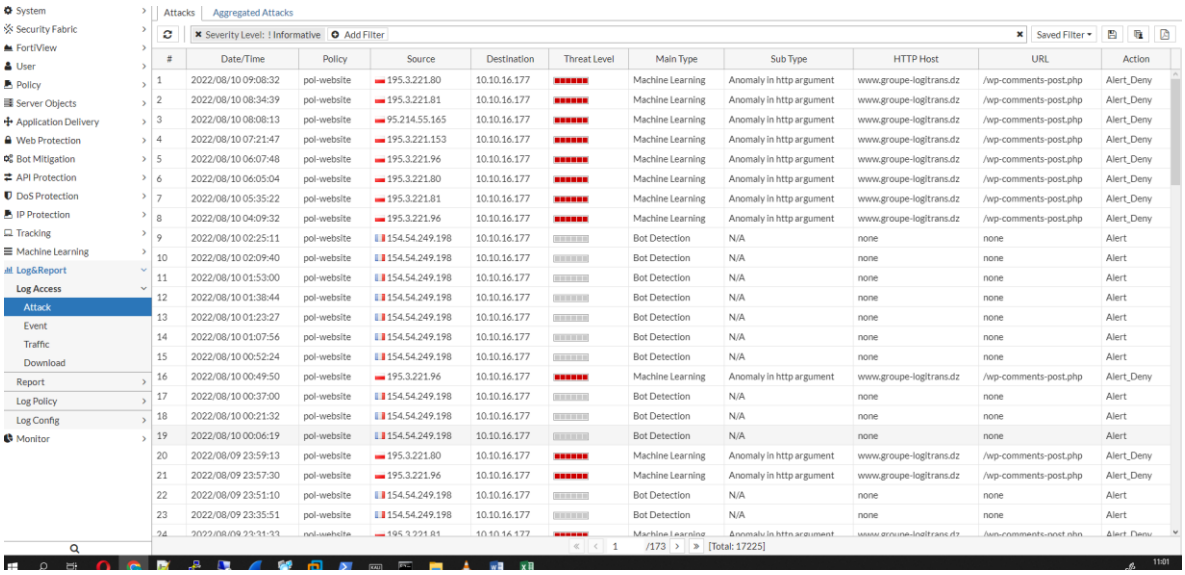

Figure 47 : Journal de capture des attaques.

4.7 Conclusion

Nous avons abordé dans ce chapitre aspect pratique de notre travail avec l'utilisation réel des matérielles informatiques.

On commence avec l'histoire de la Fortinet, par la suite on a fait une description générale de la fonctionnalité de la Fortinet. L'installation du Fortinet, et enfin quelque démonstration de l'utilisation de la FortiWeb.

Conclusion générale

De nos jours, la sécurité informatique est quasi-indispensable pour le bon fonctionnement d'un réseau, aucune entreprise ne peut prétendre vouloir mettre en place une infrastructure réseau, quel que soit sa taille, sans envisager une politique de sécurité [26].

Les firewalls représentent uniquement un outil de sécurisation, ils ne peuvent en aucun cas rendre un système ultra-sécurisé en couvrant toute ces failles, pour cette raison et afin d'augmenter le degré de sécurité d'un système, il faut installer tous les dispositifs connus comme le antivirus, les firewalls, les IDS, les antispyware, …. Etc. ces derniers constituent les éléments essentiels d'une politique global de sécurité [27].

Dans ce mémoire nous avons étudiés le réseau de la société LogiTrans, nous avons fait le « Déploiement et test d'un pare-feu Fortinet ».

Notre objectif est de mettre à la différence entre l'utilisation la configuration classique de firewall dans le monde réel comme illustrer dans le chapitre 3, avec l'utilisation de la nouvelle génération de Firewall de Fortinet nous facilite le travail, détection et utilisation de manière générale.

Nous avons conclu que la Fortinet a facilité l'utilisation et la configuration de la sécurité dans notre entreprise à travers la plateforme comme la configuration de firewall FortiGate et FortiWeb, contrairement à l'utilisation le Packet tracer. Sa rendre le travail plus complique et difficile lors de la configuration de chaque partie et plus précisément lors de la configuration de firewall Cisco.

Ce projet nous appris une grande expérience, nous avons énormément appris sur le plan de la sécurité technologique mais aussi en termes d'organisation du projet. En outre, ce projet a été une bonne occasion pour s'habituer à la vie au sein de l'entreprise, qui est très différente du climat dans les établissements universitaires.

Malheureusement nous n'avons pas fait l'édition des documents à cause du temps sont très serers et trop difficiles à manipuler les documents PDF, comme la signature dans les documents. On aura pu faire une illustration réelle avec une attaque réelle vers notre firewall Fortinet comme la fameuse attaque par déni de service(DDoS), Chevalier de Troie (Trojan), Script intersite (XSS), Injection SQL, La force brute ou …etc.

Enfin, nous espérons que notre projet puisse répondre aux besoins et satisfaire le client en particulier la direction des gestions des archives des dossiers au sein de l'entreprise LogiTrans. Donc nous le laissons avec des perspectives ouvertes

Références

[1] Concepts Pare-Feu Firewall consulte en mars 2022.

[2] Analyse conceptuelle d'une politique de sécurité dans un réseau d'entreprise. Cas de l'institut national de sécurité sociale I.N.S.S /Katanga pool consulte en mars 2022.

[3] Comparatif : quel pare-feu (firewall) choisir pour Windows en 2022 ? consulte en mars 2022.

[4] Top 8 des meilleurs logiciels de pare-feu pour Windows 10 consulte en avril 2022.

[5] Meilleur pare-feu open-source pour protéger et contrôler le trafic réseau consulte en avril 2022.

[6] Fortinet, solution de cyber-sécurité pour votre entreprise consulte en avril 2022.

[7] What is DCI?, Ciena, consulte en juin 2022.

[8] sb powering advanced research with scalable robust security, Fortinet, consulte en juin 2022.

[9] Cisco Firepower 1000 Series Data Sheet, Cisco consulte en juin 2022.

[10] Fortinet. consulte en Septembre 2022.

[11] Horizon Tech consulte en juillet 2022.

[12] FortiWeb, le pare-feu pour applications Web de Fortinet, intègre le machine learning pour détecter les menaces selon des critères comportementaux consulte en juillet 2022.

[13] FortiWeb consulte en juillet 2022.

[14] Utilisation Packet Tracer consulte en juillet 2022.

[15] Dynamic Host Configuration Protocol (DHCP) consulte en juillet 2022.

[16] Traduction d'adresses réseau (NAT) - Forum aux questions consulte en juillet 2022.

[17] Web filtering using quotas consulte en juillet 2022.

[18] FortiWeb : Pare-feu d'application web et protection des API consulte en juillet 2022.

[19] Jean-Françoispillou, tout sur les réseaux et internet,2007. consulte en Aout 2022.

[20] Qu'est-ce qu'un réseau informatique ? consulte en Aout 2022.

[21] Gen Firewall Platform consulte en Aout 2022.

[22] Fortinet consulte en Aout 2022.

[23] Tour d'horizon sur les Pare-feu nouvelle-génération FORTINET (NGFW) consulte en Aout 2022.

[24] Fortinet FortiGate pare-feux consulte en Aout 2022.

[25] Cisco Firewalls consulte en Aout 2022.

[26] Proposition et Implémentation d'un Protocole D'authentification Unique, KHERBACHE Meriem et LETAT Zina, consulte en Aout 2022.

[27] Étude et conception d'un Firewall, BELALIA Mohamed Cherif et NAACHE Khaled, consulte en Aout 2022.

[28] How does a firewall work ?, consulte en Septembre 2022.

[29] Next-Generation Firewall, consulte en Septembre 2022.

[30] Environnement de la société, consulte en Septembre 2022.