الجمهورية الجزائرية الديمقراطية الشعبية

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

وزارة التعليم العالي و البحث العلمي

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جامعة أبي بكر بلقايد – تلمسان –

Université Aboubakr Belkaïd – Tlemcen –

Faculté de TECHNOLOGIE

MEMOIRE

Présenté pour l'obtention du **diplôme** de **MASTER**

En : Télécommunication

Spécialité : Réseaux et Télécommunications

Par : Rabah Mohammed Yacine & Slimane El Mehdi

Sujet

Cadre de cyber-sécurité basé sur les pare-feux de nouvelle génération FortiGate (NGFW)

A Cybersecurity Framework based on FortiGate Next-Generation Firewalls (NGFWs)

Soutenu publiquement, le 30/06/2025 , devant le jury composé de :

Mme BENLALDJ Lamia	MCB	Université de Tlemcen	Présidente
Mme OTMANI Amina	MCB	Université de Tlemcen	Examinateur
Mme SLIMANE Zohra	Professeur	Université de Tlemcen	Encadreur
M ABDELMALEK Abdelhafid	MCB	Université de Tlemcen	Co-Encadreur

Année universitaire : 2024/2025

Dédicace

« Au nom de Dieu, le clément, le miséricordieux. Gloire à Allah Maître des mondes, que la prière de Dieu soit sur son prophète Mohamed (q.s.s.l) sur sa famille et tous ses compagnons »

Je dédie ce travail à :

Ma très chère mère qui a été toujours à mes côtés et qui me donne que le Soutien, beaucoup d'amour, le courage pour avoir cette réussite et bien sûr à mon père qui a été la source de ma volonté, ainsi qu'à ma grand-mère, qui prie toujours pour moi dans ses prières.

A

Mes frères

Ma sœur

Mes oncles

Mes tantes

Mohammed

Dédicace

« Au nom de Dieu, le clément, le miséricordieux. Gloire à Allah Maître des mondes, que la prière de Dieu soit sur son prophète Mohamed (q.s.s.l) sur sa famille et tous ses compagnons »

Je dédie ce mémoire :
A ma famille, elle qui m'a doté d'une éducation digne, son amour a fait de moi ce que je suis aujourd'hui.

A ma très chère Maman

Quoi que je fasse ou que je dise, je ne saurai jamais te remercier comme il se doit. Ton affection me couvre, ta bienveillance me guide et ta présence à mes cotés a toujours été ma source de force pour affronter les différents obstacles.

A mon très cher Père

Tu as toujours été à mes côtés pour me soutenir et m'encourager. Je voudrais te remercier pour ton amour, ta générosité, ta compréhension. Ton soutien fut une lumière dans tout mon parcours. Aucune dédicace ne saurait exprimer l'amour, l'estime et le respect que j'ai toujours eu pour toi.
À tous ce que j'aime et qui m'aiment.
À tous mes amis.
Merci.

El Mehdi

Résumé

Dans le cadre de ce projet de fin d'études, nous avons entrepris un travail d'installation, de configuration et de test d'un pare-feu de nouvelle génération FortiGate, une solution de sécurité développée par l'entreprise Fortinet. FortiGate figure parmi les pare-feu réseau les plus largement déployés au niveau mondial. Il offre un large éventail de fonctionnalités avancées en matière de sécurité et de connectivité, réunies au sein d'une plateforme unifiée, centralisée via FortiGate Cloud.
L'objectif principal de ce projet était de mettre en place une plateforme de test virtuelle capable de simuler un environnement réseau réaliste, intégrant divers équipements, dans le but d'expérimenter et de valider plusieurs politiques de sécurité.
Les tests réalisés à l'aide d'une licence d'évaluation se sont révélés globalement très satisfaisants. Pour explorer l'ensemble des fonctionnalités avancées (filtrage d'applications et de contenus, VDOM, VPN IPsec/SSL, SD-WAN, inspection SSL, sandboxing, etc.), l'acquisition d'une licence complète permettrait de réaliser des tests plus représentatifs des usages réels en entreprise.
Ce projet nous a ainsi permis, d'une part, de renforcer nos compétences pratiques en sécurité informatique et en administration réseau, et d'autre part, de mieux appréhender les enjeux concrets de la cybersécurité.

Mots clés :
Cybersécurité, Attaque, Vulnérabilité, VMware, Eve-ng, Fortigate, NGFW, Pare-feu nouvelle génération, Proxy, DMZ, Filtrage

Abstract

As part of this final-year project, we undertook the installation, configuration, and testing of a next-generation firewall, FortiGate, a security solution developed by Fortinet. FortiGate is one of the most widely deployed network firewalls worldwide. It offers a broad range of advanced security and connectivity features, all integrated into a unified platform, centrally managed through FortiGate Cloud.
The main objective of this project was to set up a virtual testing platform capable of simulating a realistic network environment, integrating various devices, in order to experiment with and validate multiple security policies. The tests carried out using an evaluation license proved to be overall very satisfactory. However, to fully explore the set of advanced features (such as application and content filtering, VDOM, IPsec/SSL VPN, SD-WAN, SSL inspection, sandboxing, etc.), acquiring a full license would allow for more representative testing of real-world enterprise use cases.
This project has thus enabled us, on the one hand, to strengthen our practical skills in cybersecurity and network administration, and on the other hand, to gain a better understanding of the real-world challenges of cybersecurity.

Keywords : Cybersecurity, Attack, Vulnerability, VMware, Eve-ng, Fortigate, NGFW, Next generation Firewall, Proxy, DMZ, Filtering

ملخص

في إطار هذا مشروع نهاية الدراسة، قمنا بعمل يتضمن تثبيت، إعداد واختبار جدار حماية من الجيل الجديد FortiGate. وهو حل أمني مطور من قبل شركة Fortinet.

يُعتبر FortiGate من بين أكثر جدران الحماية انتشارًا على مستوى العالم.

حيث يقدم مجموعة واسعة من الميزات المتقدمة في مجال الأمان والاتصال، مدمجة ضمن منصة موحدة ومركزة تُدار عبر FortiGate Cloud.

الهدف الرئيسي من هذا المشروع هو إنشاء منصة اختبار افتراضية قادرة على محاكاة بيئة شبكة واقعية، تتضمن أجهزة مختلفة، من أجل تجربة وتقييم عدة سياسات أمنية قد أظهرت الاختبارات التي تم إجراؤها باستخدام رخصة تقييم نتائج مرضية بشكل عام.

ولاستكشاف كافة الميزات المتقدمة (مثل تصفية التطبيقات والمحتوى، VPN IPsec/SSL، VDOM ، SD-WAN ، sandboxing SSL ، وغيرها فإن اقتناء رخصة كاملة من شأنه أن يُتيح إجراء اختبارات أكثر تمثيلاً للاستخدامات لحقيقية في بيئة المؤسسات.

هذا المشروع أتاح لنا، من جهة، تعزيز مهاراتنا التطبيقية في مجال أمن المعلومات وإدارة الشبكات، ومن جهة أخرى، فهمًا أعمق للتحديات الحقيقية للأمن السيبراني

الكلمات المفاتيح :

الأمن السيبراني، الهجوم الإلكتروني، الثغرات الأمنية، جدار الحماية من الجيل التالي، البروكسي، المنطقة منزوعة السلحً، التصفية DMZ، NGFW، Fortigate، Eve-ng، VMware

Remerciements

Avant tout, nous remercions ALLAH Le Tout Puissant qui nous à donner la force et surtout la patience d'arriver au bout de notre travail.

Du fond du cœur nous remercions nos chers parents qui nous ont toujours guidés, encouragés et qui ont fait de leur mieux pour que puissions réussir nos projets.

Nous remercions notre encadreur Mme SLIMANE Zohra et notre co-encadreur Mr ABDELMALEK Abdelhafid pour leur aide tout au long de notre travail. Comme nous tenons à les remercie pour leurs encouragements, leur soutien et leurs précieux conseils et orientations.

Nous sommes particulièrement sensibles à l'honneur que nous font les membres du jury en acceptant de lire et de juger ce mémoire. Nous les remercions sincèrement pour le temps qu'ils ont consacré à la lecture et l'évaluation de notre travail. Nous tenons à remercier tout particulièrement Madame BENLALDJ Lamia d'avoir accepté de présider ce jury. Nous remercions également Mme OTMANI Amina en tant qu'examinatrice. Leurs compétences élèvent considérablement la valeur de ce travail.

Nos remerciements s'adressent aussi à tous les enseignants du département Télécommunication, et particulièrement aux enseignants du parcours Master Réseaux et Télécommunications. Veuillez, Mesdames et Messieurs, trouver dans ce travail une reconnaissance sincère pour tout le savoir que vous nous aviez prodigué tout au long de notre cursus avec autant de dynamisme, de compétence et de rigueur.

Bien entendu, il nous serait impossible de terminer sans adresser une pensée chaleureuse aux ingénieurs de Sonatrach Activité LQS Oran, au sein duquel nous avons effectué notre stage dans le cadre de ce projet de fin d'études. Un grand merci à toutes les personnes qui ont rendu notre expérience de stage mémorable et fructueuse par leur accueil chaleureux, leur soutien et leur collaboration.

Table des matières

CHAPITRE III

Méthodologie de test: Emulation avec Eve-ng Installation et Configuration

CHAPITRE IV

Déploiement de Fortigate Firewall : Configuration et scénarios de tests de validation

Liste des figures

Figure **page**

Figures **page**

Figures **page**

Liste des tableaux

Tableau **Page**

Acronymes

5GE	5G Evolution
AES	Advanced Encryption Standard
AI	Artificial Intelligence
API	Application Programming Interface
APT	Advanced Persistent Threat
ARP	Address Resolution Protocol
AWS	Amazon Web Services
CASB	Cloud Access Security Broker
CCNA	Cisco Certified Network Associate
CCNP	Cisco Certified Network Professional
CLI	Command Line Interface
CN	Common Name
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DGA	Domain Generation Algorithm
DNS	Domain Name System
EVE-NG	Emulated Virtual Environment – Next Generation
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
ICMP	Internet Control Message Protocol

IDS	Intrusion Detection System
IOL	IOS On Linux
IoT	Internet of Things
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
KVM	Kernel-based Virtual Machine
L2TP	Layer 2 Tunneling Protocol
MAC	Media Access Control
MFA	Multi-Factor Authentication
MitM	Man-in-the-Middle
NGFW	Next Generation Firewall
OVA	Open Virtual Appliance
OT	Operational Technology
QEMU	Quick Emulator
RSA	Rivest–Shamir–Adleman
SaaS	Software as a Service
SASE	Secure Access Service Edge
SD-WAN	Software-Defined Wide Area Network
SHA	Secure Hash Algorithm
SFTP	SSH File Transfer Protocol
SMC	Security Management Center
SnortML	Snort + Machine Learning
SP5	Security Processor 5
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security

UDP	User Datagram Protocol
VDOM	Virtual Domain
VM	Virtual Machine
VPC	Virtual Private Cloud
VPN	Virtual Private Network
XSS	Cross-Site Scripting
ZTNA	Zero Trust Network Access

Introduction générale

Le spectaculaire développement des technologies de l'information et de la communication a radicalement transformé nos modes de vie, notre environnement professionnel et nos systèmes économiques. En ce sens, les réseaux informatiques sont devenus le socle de nos infrastructures contemporaines. Mais cette montée en puissance croissante vers les systèmes connectés est accompagnée d'une hausse sensible des risques et des menaces numériques. Les attaques de la composante numérique se diversifient, sont plus complexes et plus banales, visent à la fois les particuliers que les grands acteurs. Les intrusions malsaines, les malwares, les attaques par déni de service (DoS), ou encore les menaces persistantes avancées (APT) constituent des menaces qui déstabilisent la sécurité des systèmes d'information.

Face à cette réalité, la cybersécurité s'est promis d'être un domaine stratégique et d'urgence. Elle regroupe l'ensemble des moyens, techniques et procédés visant à protéger les systèmes informatiques, les réseaux et les données contre les accès non autorisés, les altérations et les destructions. Parmi les dispositifs de sécurité réseau les plus utilisés, les pare-feux de nouvelle génération jouent un rôle central. Ils ne servent pas seulement à filtrer le trafic réseau, mais aussi à repérer et à prévenir les activités anormales à l'aide de fonctions intégrées comme l'inspection en profondeur des paquets, la prévention des intrusions (IPS), la gestion des applications ou même l'analyse du trafic chiffré.

Dans le cadre de ce projet de fin d'études, nous avons choisi de travailler sur l'installation, la configuration et le test d'un pare-feu FortiGate, une solution développée par l'entreprise Fortinet, reconnue pour ses performances en matière de sécurité réseau. L'objectif principal est de mettre en place une plateforme de test virtuelle permettant de simuler un environnement réseau réel, d'y intégrer différents équipements, et d'expérimenter diverses politiques de sécurité.

Pour cela, plusieurs étapes ont été suivies. Nous avons d'abord installé VMware Workstation, un hyperviseur permettant de créer des machines virtuelles. Ensuite, nous avons utilisé EVE-NG (Emulated Virtual Environment – Next Génération), un outil puissant de simulation de topologies réseau, dans lequel nous avons importé et intégré les images des équipements nécessaires. Avec l'aide de FileZilla et WinSCP, nous avons été en mesure de transférer les

fichiers depuis la machine locale vers le site distant et ainsi mettre facilement en place les composants dans l'environnement EVE-NG. En dernier lieu, nous avons mis en place le pare-feu FortiGate, téléchargé à partir du site officiel de Fortinet, et nous l'avons ajouté à notre infrastructure virtuelle pour effectuer des tests de configuration et d'évaluation.
Ce projet nous a, d'une part, donné l'occasion de renforcer nos compétences pratiques en sécurité informatique et en administration réseau, mais d'autre part de mieux saisir les enjeux concrets de la cyber-sécurité.

La suite de ce mémoire est organisée de la façon suivante. Dans le premier chapitre « Cyber-sécurité-Etat de l'art », nous traitons d'abord des notions de base liées à la cybercriminalité et aux mécanismes de défense associés, nous mettons ensuite en lumière dans le chapitre deux, les solutions de sécurité basées sur les pare-feux nouvelle génération, avant de décrire dans le chapitre trois les différentes étapes techniques de mise en place de la plateforme d'émulation sous Eve-ng, jusqu'aux scénarios de tests réalisés avec le pare-feu FortiGate qui seront présentés dans le chapitre quatre.

Chapitre 1

Cyber-sécurité

Etat de l'art

1

Cyber-sécurité - Etat de l'art

I.1 Introduction

Le paysage contemporain des réseaux, caractérisé par une évolution rapide, est confronté à une pléthore de menaces multiformes, notamment des intrusions dans les systèmes et des infections par des logiciels malveillants, ainsi que des mécanismes d'attaque automatisés tels que des vers, des virus, des chevaux de Troie et des attaques par déni de service (Dos). Selon les prévisions, environ 25 milliards de tentatives d'accès non autorisées se produisent chaque jour dans le monde, un phénomène qui semble s'intensifier de manière persistante. Des outils tels que les systèmes de détection d'intrusion (IDS), les systèmes de prévention des intrusions (IPS) et les pare-feu sont utilisés pour examiner et évaluer les activités associées au trafic réseau. Néanmoins, la prévalence des techniques de chiffrement et des protocoles d'anonymat exacerbe considérablement les difficultés liées à l'identification, à la neutralisation et à la détection des cyberattaques.

Dans ce chapitre, nous examinerons les différentes facettes de la cyber sécurité, notamment les principales menaces et cyberattaques, les stratégies de protection recommandées pour les utilisateurs.

I.2 Cybercriminalité

I.2.1 Définition

La cybercriminalité est un terme utilisé pour désigner l'ensemble des infractions commises à l'aide des technologies numériques, des systèmes informatiques et d'Internet. Bien qu'il ne possède pas de définition légale universelle, il est généralement compris comme incluant tous les crimes facilités ou réalisés par des appareils électroniques et des réseaux informatiques.

Certaines définitions sont plus larges et englobent toute activité criminelle liée à la technologie, tandis que d'autres se limitent aux délits visant l'acquisition ou la manipulation d'informations à des fins personnelles [1].

I.2.2 Vulnérabilités

Une vulnérabilité est une faille dans un système informatique, logiciel ou matériel, qui peut être exploitée afin de compromettre la sécurité [2]. La vulnérabilité se présente sous différentes formes, mais les plus courantes sont les suivantes :

Vulnérabilités logicielles : Les vulnérabilités logicielles sont des défauts ou des imperfections d'un logiciel qui peuvent être exploités par des acteurs malveillants pour compromettre la sécurité des systèmes, des applications ou des réseaux. Ces vulnérabilités peuvent provenir d'erreurs de codage, de méthodologies de programmation inadéquates ou d'une validation d'entrée insuffisante, et elles peuvent faciliter des attaques qui incluent l'exécution de code nuisible, l'exfiltration non autorisée de données ou la prise de contrôle complète de systèmes compromis [3]-[5].

Vulnérabilités d'authentification : les vulnérabilités d'authentification indiquent des déficiences ou des lacunes inhérentes aux cadres d'authentification des systèmes logiciels, des réseaux ou des applications, qui peuvent être exploitées par des acteurs malveillants pour obtenir un accès non autorisé à des informations confidentielles ou à des ressources critiques [6].

Vulnérabilités de configuration : les vulnérabilités de configuration proviennent d'insuffisances imputables à des configurations erronées ou incomplètes de systèmes, de logiciels ou d'appareils réseau. Ces vulnérabilités se manifestent généralement lorsqu'un système est initialisé avec des configurations par défaut, des ports ouverts superflus, des services non sécurisés ou une gouvernance insuffisante des droits d'accès [7].

Vulnérabilités physiques : Les vulnérabilités physiques concernent des déficiences associées à un accès physique non autorisé à des appareils informatiques (y compris des serveurs, des postes de travail, des périphériques réseau, etc.), qui peuvent aboutir au vol, à la destruction, à l'altération ou à la compromission de données ou de systèmes. Ces vulnérabilités incluent l'absence de contrôles d'accès physiques, un placement sous-optimal des équipements et des mesures de surveillance insuffisantes [8].

Vulnérabilités réseau : Les vulnérabilités du réseau représentent des déficiences ou des insuffisances dans l'architecture, l'exécution ou la supervision d'un réseau informatique qui peuvent être exploitées par des adversaires pour accéder illégalement à des données, en perturber les opérations ou les exfiltrer [9].

Vulnérabilités matérielles : les vulnérabilités matérielles désignent les faiblesses inhérentes aux composants tangibles d'un système informatique (tels que les unités centrales ou la mémoire), qui peuvent être exploitées pour obtenir un accès non autorisé à des données confidentielles ou perturber le fonctionnement du système [10].

Vulnérabilités liées à l'architecture et au design : Les vulnérabilités liées à l'architecture et à la conception désignent des failles introduites lors de la phase de conception d'un système, d'une application ou d'un réseau. Ces vulnérabilités résultent de décisions structurelles inadéquates ou de cadres de sécurité incomplets et peuvent être exploitées indépendamment des déficiences de codage ou des erreurs de configuration [11].

Vulnérabilités (API) Les vulnérabilités de l'interface de programmation d'applications (API) représentent des failles de sécurité inhérentes à la conception, au développement ou à la gouvernance des API. Ces vulnérabilités peuvent être exploitées par des acteurs malveillants pour contourner les mesures de sécurité, accéder illégalement à des informations sensibles, perturber les services ou introduire du code nuisible. Les exemples typiques incluent des mécanismes d'authentification ou d'autorisation inadéquats, une exposition excessive des données ou des injections de code telles que SQL ou XSS via des configurations d'API [12].

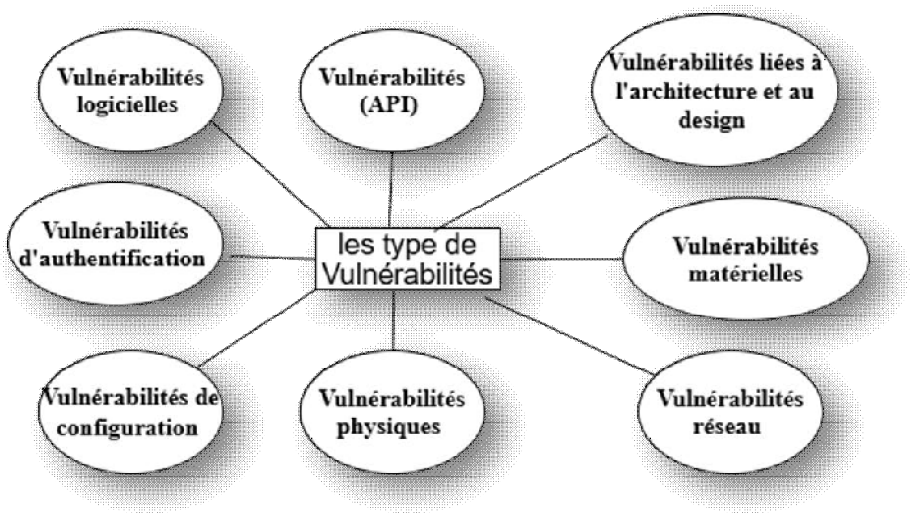


Figure 1.1 : Différents types de vulnérabilité.

I.3 Cyberattaques

Une cyberattaque constitue l'exploitation intentionnelle de systèmes informatiques, d'entreprises et de réseaux dépendant de la technologie. Les cyberattaques utilisent un code malveillant pour modifier la programmation, la logique ou les données informatiques, ce qui entraîne des conséquences perturbatrices susceptibles de compromettre l'intégrité des données et de faciliter la cybercriminalité, notamment l'usurpation d'informations et d'identité. Une cyberattaque est également appelée attaque de réseau informatique [13].

I.3.1 Attaques par ingénierie sociale

Des tentatives de manipulation psychologique sont utilisées par les agresseurs pour inciter les individus à divulguer des informations confidentielles, à accorder un accès non autorisé aux systèmes ou à se livrer à des activités compromettantes. Ces attaques sont fondées sur l'exploitation de la confiance, de la peur ou de la curiosité des victimes, au lieu de s'appuyer uniquement sur des méthodologies techniques [14]**.**

- **Phishing (Hameçonnage) :** e-mails frauduleux imitant des entités de confiance.
- **Spears phishing :** phishing ciblé sur une personne ou organisation spécifique.
- **Pretexting :** création d'un faux scénario pour obtenir des infos confidentielles.
- **Baiting (appât) :** promesse d'un avantage (ex. : téléchargement gratuit) pour infecter le système.

I.3.2 Attaques logicielles

Les attaques logicielles, communément appelées attaques de logiciels malveillants, désignent des activités malveillantes qui utilisent des programmes informatiques spécialement conçus pour infiltrer, endommager, perturber ou obtenir un accès non autorisé aux systèmes informatiques. Cette catégorie de logiciels englobe les virus, les vers, les chevaux de Troie, les logiciels espions et même les logiciels publicitaires. Leurs objectifs peuvent varier considérablement : ils peuvent inclure le vol de données, le sabotage, l'espionnage ou les demandes d'extorsion [15].

- **Virus** : Code malveillant qui s'attache à un fichier et se propage.
- **Ver (Worm)** : Se propage seul sans action humaine, souvent via réseau.
- **Cheval de Troie (Trojan)** : Se cache dans un logiciel légitime.
- **Ransomware** : Verrouille les données de la victime et demande une rançon.
- **Spyware** : Espionne l'activité de l'utilisateur (ex. mots de passe, frappes clavier).
- **Adware** : Inonde l'utilisateur de publicités indésirables.
- **Keylogger** : Enregistre tout ce que l'utilisateur tape au clavier.

I.3.3 *Attaques réseau*

Les attaques réseau sont des actes intentionnels conçus pour perturber, intercepter, modifier ou empêcher le fonctionnement normal d'un réseau informatique. Ces attaques se concentrent sur les données en transit, les appareils interconnectés ou les protocoles de communication dans le but d'exproprier des informations, de provoquer des dysfonctionnements ou de compromettre la sécurité globale du réseau [16].

- **Attaque par déni de service (Dos/DDoS)** : Saturation d'un serveur ou réseau avec un flux massif de requêtes pour le rendre inaccessible.
- **Man-in-the-Middle (MitM)** : L'attaquant intercepte la communication entre deux parties pour espionner ou modifier les échanges.
- **Sniffing / Écoute réseau :** Capture du trafic réseau pour collecter des données sensibles (ex : identifiants, mots de passe).
- **Spoofing (usurpation)** : Détournement de trafic en falsifiant une adresse IP (IP spoofing), MAC, ou DNS.
- **Replay Attack** : Réutilisation d'une transmission interceptée pour tromper un système (ex : relecture d'un mot de passe capturé).

I.3.4 Attaques sur les identifiants / authentification

Les attaques liées aux informations d'identification et à l'authentification ciblent spécifiquement les mécanismes de connexion afin d'obtenir illégalement un accès à des systèmes ou à des comptes. Leurs objectifs incluent le vol, la devinette ou la réutilisation des informations d'identification d'un utilisateur (identifiant/mot de passe) [16].

- **Brute force :** Test de toutes les combinaisons possibles pour deviner un mot de passe.
- **Credential stuffing** : Réutilisation de mots de passe volés sur d'autres comptes.
- **Keylogging :** Enregistrement des frappes clavier pour capter des mots de passe.

I.4 Cyber-sécurité

Le sécurité cybernétique est la pratique visant à protéger les appareils électroniques, les réseaux et les informations sensibles contre l'accès non autorisé, le vol, les dommages ou les perturbations. Elle repose sur une combinaison de contrôles techniques, administratifs et physiques afin d'assurer la confidentialité, l'intégrité et la disponibilité des données. Plus globalement, la cyber sécurité regroupe un ensemble de pratiques destinées à protéger les

systèmes informatiques et les réseaux contre toute intrusion, utilisation abusive, divulgation, modification ou destruction non autorisée. Elle permet également de lutter contre diverses menaces numériques telles que les virus, les logiciels malveillants et le piratage. Pour cela, elle nécessite la mise en place de technologies, de processus et de politiques adaptées afin de prévenir les cyberattaques et de garantir la protection des actifs numériques [18].

I.4.1 Service de sécurité

Dans le contexte actuel d'une société numérique aux multiples facettes, les agents de communication peuvent être localisés sur de grandes distances, en grande partie grâce à l'émergence d'Internet. Les infrastructures utilisées pour faciliter les connexions entre ces agents présentent divers degrés de qualité de service en termes de rapidité, de fiabilité et de confidentialité. En effet, la prévalence et l'importance des transactions d'informations augmentent, ce qui rend la sauvegarde de ces interactions de la plus haute importance.

Le domaine de la sécurité informatique concerne la sauvegarde des actifs matériels et logiciels d'une organisation, garantissant ainsi que leur utilisation soit strictement conforme aux objectifs fixés. D'une manière générale, ce domaine vise à soutenir trois services de sécurité principaux, qui sont définis comme suit [4].

- **Confidentialité :** Le concept de confidentialité postule que les informations conservées par une entité signifient que l'accès aux données présentes sur le réseau ou au trafic du réseau est réservé aux seules personnes qui ont reçu les autorisations appropriées. Aucune personne n'est autorisée à accéder à l'information à moins de posséder les droits requis pour le faire. Le processus d'identification des utilisateurs nécessite la mise en œuvre de mécanismes d'authentification. La protection des informations contre tout examen non autorisé nécessite l'utilisation de techniques de cryptage [12].
- **Intégrité : :** L'intégrité est définie comme l'assurance que les méthodologies de gestion des données garantissent le traitement précis de ces informations sans aucune anomalie. Les données ne doivent pas être modifiées pendant la transmission et le stockage. Aucune personne ne doit avoir la capacité de modifier le contenu des informations ou des fichiers associés. De plus, le fait de supprimer de telles informations est encore moins acceptable. Pour préserver l'intégrité des données, il est impératif que l'expéditeur soit authentifié en permanence [17].

- **La disponibilité** : Objectif de sécurité visant à garantir un accès constant aux données et aux services fournis par le système d'information. C'est une assurance de la persistance des services ainsi que de l'efficacité des applications, du matériel et de l'environnement de l'organisation [3].

I.4.2 Mesures de la sécurité

Pour renforcer la cybersécurité, il est essentiel de mettre en œuvre un ensemble de mesures de sécurité appropriées telles que les pare-feux, les réseaux privés virtuels (VPN), les antivirus, les IDS, etc

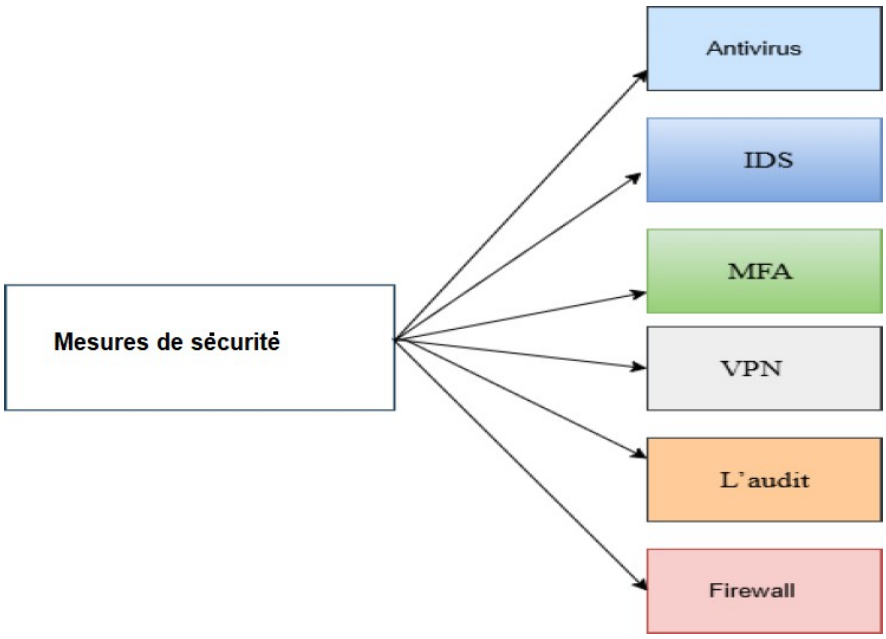


Figure 1.2 : les mesures de sécurité

I.4.2.1 Logiciel antivirus

Les programmes antivirus sont des applications logicielles sophistiquées conçues pour détecter, neutraliser et éradiquer les logiciels nuisibles (les virus ne représentent qu'un exemple) qui capitalisent sur les vulnérabilités des systèmes de sécurité. [19].

Un logiciel antivirus représente une application de protection que vous intégrez sur un ordinateur ou un appareil mobile afin de prévenir toute contamination par des logiciels nuisibles. Ce programme a la capacité de :

- Identifier et éliminer les virus présents sur un disque.

- Vérifier la présence de virus et, si nécessaire, nettoyer et supprimer les fichiers compromis.
- Ils examinent tous les emplacements où un virus pourrait s'installer, y compris la mémoire et les supports de stockage qui peuvent se trouver sur le réseau.

I.4.2.2 Système de détection d'intrusion (IDS)

Un système destiné à détecter des intrusions, connu sous le nom de Système de Détection d'Intrusions (ou IDS), est conçu pour identifier des comportements anormaux ou douteux sur l'entité surveillée, qu'il s'agisse d'un réseau ou d'un appareil. Cela offre une visibilité sur les tentatives d'intrusion, qu'elles soient réussies ou infructueuses. On distingue principalement deux catégories d'IDS :

- Les N-IDS, qui fournissent une protection au niveau du réseau.
- Les H-IDS, qui garantissent la sécurité au niveau des dispositifs. [19].

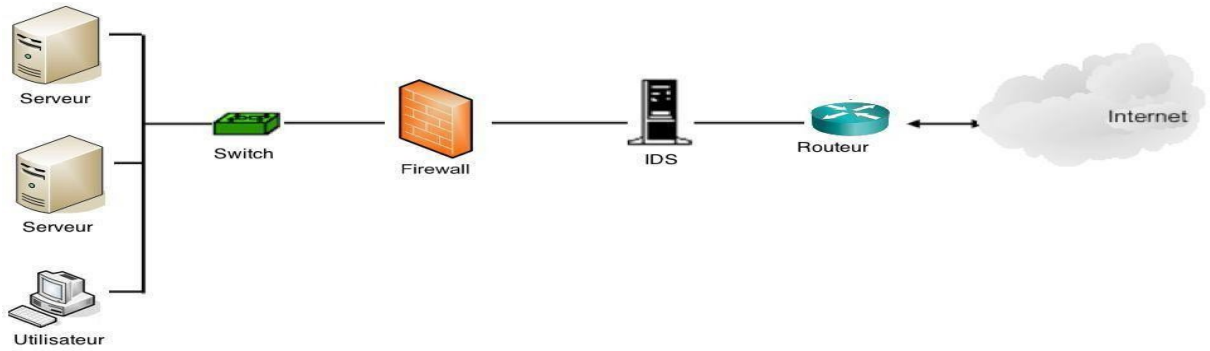


Figure 1.3 : Exemple d'un IDS dans un réseau.

I.4.2.3 Authentication multifacteur (MFA)

L'authentification multifacteur est une méthode de sécurité qui exige au moins deux preuves différentes (facteurs) pour vérifier l'identité d'un utilisateur.

I.4.2.4 Réseau virtuel privé(VPN)

Un Réseau Privé Virtuel, abrégé « VPN » pour Virtuel Private Network, désigne l'application du protocole IPSec pour établir un tunnel de communication sécurisé à des fins privées, dans un réseau public qui n'est pas protégé. Il est mis en place par une entreprise pour relier ses divers sites par le biais d'Internet, afin de garantir la sécurité des informations échangées [20]. Ce réseau offre deux avantages majeurs :

- De hautes performances en termes de bande passante, autrement dit des communications à très haut débit et de très grande qualité.
- La sécurité et la confidentialité des données.

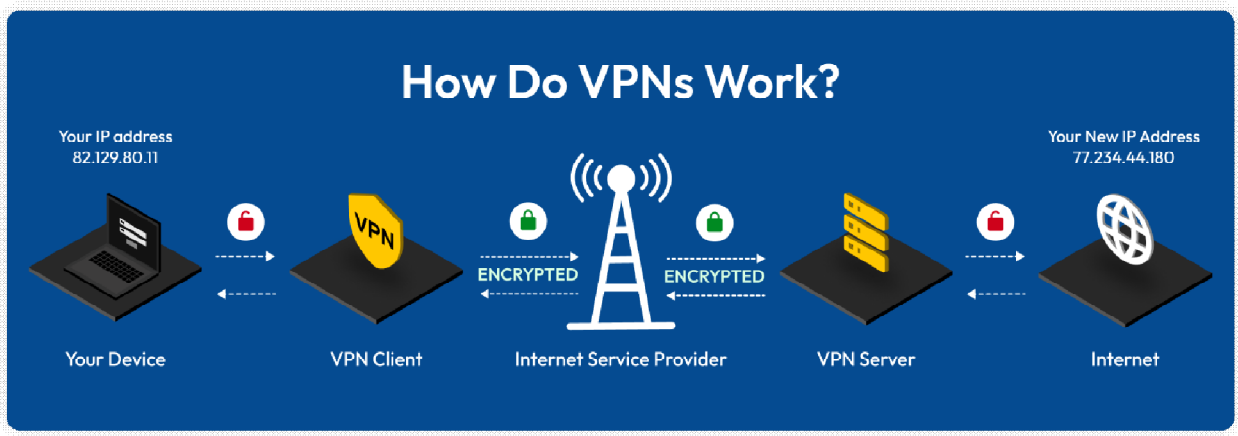


Figure 1.4 : Fonctionnement de VPN [20]

I.4.2.5 Cryptographie

La cryptographie est un pilier essentiel de la cybersécurité moderne. Elle utilise des algorithmes et des techniques avancées pour sécuriser les données, que ce soit en transit ou au stockage, et joue un rôle crucial dans la prévention des cyberattaques et la protection des données sensibles, en s'appuyant sur des techniques de chiffrement, d'authentification et de signature. Des algorithmes comme RSA (chiffrement asymétrique) et AES (chiffrement symétrique), ainsi que des fonctions de hachage comme SHA, sont des outils essentiels dans ce domaine. [20]

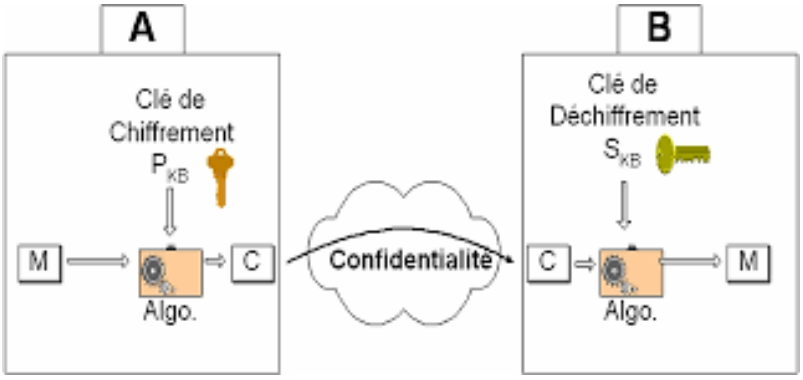


Figure 1.5 : Exemple d'application de la cryptographie (chiffrement asymétrique)

I.4.2.6 L'audit

L'audit représente une méthode d'analyse autonome et structurée qui sert à examiner la sécurisation des systèmes d'information d'une entreprise. Son but est de déceler les faiblesses, évaluer les menaces potentielles, s'assurer du respect des régulations telles qu'ISO 27001 et vérifier l'efficacité des dispositifs de sécurité établis.

Le but est de garantir la protection, la cohérence et l'accessibilité des informations et des systèmes, tout en fournissant des suggestions pour renforcer la sécurité de manière globale [21].

I.4.2.7 Pare-feu (Firewall)

Le pare-feu est un dispositif logiciel et/ou matériel qui contribue à l'application de la politique de sécurité d'un réseau, laquelle détermine les catégories de communication permises sur ce réseau informatique. Il évalue la protection des applications et des données [19].

I.5 Conclusion

Dans ce chapitre, nous avons souligné la nécessité de la sécurité numérique, qui est devenue une composante essentielle de notre quotidien. Nous avons aussi exposé les stratégies de défense en matière de cyber sécurité.

Parmi les mesures de sécurité dont nous avons parlé, le firewall constitue un pilier fondamental, nous aborderons ce dernier dans le chapitre suivant, en détaillant son champ d'application et en découvrant les nouvelles générations de firewall (NGFW).

Chapitre 2

Pare-feux nouvelle génération

2

Pare-feux nouvelle génération

II.1 Introduction

Comme, nous venons de le voir au chapitre précédent, afin de renforcer la cybersécurité, il est impératif de mettre en place des solutions qui renforcent la sécurité des systèmes informatiques. Parmi ces solutions, le déploiement de pare-feu (firewall) à la frontière des réseaux informatiques est l'une des plus essentielles. Agissant comme une barrière de protection pour un réseau ou un système informatique, il surveille et contrôle le trafic réseau entrant et sortant en se basant sur des règles de sécurité prédéfinies.

II.2 Pare-feux (Firewall) classiques

II.2.1 Définition

Un pare-feu classique, également appelé pare-feu traditionnel ou pare-feu de niveau réseau, est un système de sécurité réseau qui surveille et filtre le trafic entrant et sortant en se basant sur des règles prédéfinies. Son rôle principal est de protéger un réseau en bloquant ou en autorisant les communications en fonction de ces règles, qui peuvent inclure des adresses IP, des ports, des protocoles, ou l'état de la connexion. Il peut inclure une zone démilitarisée (DMZ) pour isoler certains services accessibles depuis l'extérieur [22].

II.2.2 Nécessité d'un firewall

Sans la mise en œuvre d'un pare-feu, les systèmes disparates du sous-réseau deviennent vulnérables aux attaques externes. Dans un environnement dépourvu de pare-feu, la sécurité du réseau repose principalement sur des mesures de sécurité au niveau des machines, ce qui oblige tous les machines à collaborer efficacement pour atteindre une norme de sécurité

cohérente et élevée. Plus le sous-réseau est étendu, plus il devient difficile de maintenir tous les hôtes à un niveau de sécurité équivalent. À mesure que les failles et les défaillances de sécurité deviendront de plus en plus répandues, les intrusions cesseront d'être perçues comme le résultat d'attaques complexes, mais plutôt comme la conséquence de simples oublis de configuration et de sélections de mots de passe sous-optimales. Par conséquent, il suffirait qu'un seul système hôte soit compromis pour que l'ensemble du site soit rendu vulnérable.

II.2.3 Fonctionnement d'un pare-feu

L'objectif principal d'un pare-feu est de réguler le flux d'informations qui transite entre l'ordinateur, notre réseau et Internet.

Un système de pare-feu comprend un ensemble de règles prédéfinies qui permettent :

- Soit d'autoriser uniquement les communications ayant été explicitement autorisées : "Tout ce qui n'est pas explicitement autorisé est interdit".
- Soit d'empêcher les échanges qui ont été explicitement interdits
- Le choix de l'une ou l'autre de ces méthodes dépend de la politique de sécurité adoptée par l'entreprise désirant mettre en œuvre un filtrage des communications.
- La première méthode de pare-feu est sans nul doute la plus sûre, mais elle impose toutefois une définition précise et contraignante des besoins en communication [23].

II.2.4 Avantages d'un Firewall

- Pour protéger l'ensemble de l'infrastructure réseau, le pare-feu centralise ses mesures de sécurité réseau à un moment précis.
- Il est essentiel que l'administrateur réseau évalue régulièrement le trafic pour s'assurer qu'il n'a pas contourné ou compromis le système.
- Le réseau local continuera à fonctionner efficacement en raison de la localisation de la perturbation en un seul point.

II.2.5 Inconvénients d'un Firewall

- Ses capacités de protection sont limitées aux attaques qui traversent son système.
- Une simple modification vers un autre format est nécessaire lorsque le pare-feu bloque des types de fichiers sortants. [24]

II.2.6 Principes du filtrage

En fonction de l'appareil utilisé, les données sont extraites des flux de réseau couvrant une ou plusieurs couches de 2 à 7 du modèle OSI, potentiellement liées entre elles, et juxtaposées par rapport à un ensemble prédéfini de critères de filtrage. Un état peut être maintenu pour chaque flux reconnu, ce qui facilite la gestion de la dimension temporelle grâce à un filtrage basé sur les données historiques du flux.

Les différentes classifications du filtrage sont décrites ci-dessous :

II.2.6.1 Le filtrage simple de paquet (Stateless)

Le Principe : Il s'agit de la méthode de filtrage la plus simple, fonctionnant au niveau des couches réseau et transport du modèle OSI. Actuellement, la plupart des routeurs facilitent le filtrage de base des paquets. Ce processus consiste à autoriser ou à refuser la transmission de paquets d'un réseau à un autre en fonction des critères suivants **:**

- ✓ L'adresse IP Source/Destination.
- ✓ Le numéro de port Source/Destination.
- ✓ Et bien sûr le protocole de niveaux 3 ou 4.

Cela nécessite de configurer le Firewall ou le routeur par des règles de filtrages, généralement appelées des ACL (Access Control Lists). Ces paramètres doivent être saisis par un administrateur ou le fabricant au moyen des règles qu'ils ont définies à l'avance.

Si un paquet de données présente des paramètres non considérés comme acceptables, le protocole de pare-feu sans état identifie la menace, puis restreint ou bloque les données qui l'hébergent.

Les limites: Le défi initial tient à la nécessité pour l'administrateur réseau d'autoriser rapidement un nombre excessif d'accès, compromettant ainsi la capacité du pare-feu à fournir une véritable protection. Par exemple, pour activer les connexions à Internet depuis le réseau privé, l'administrateur doit autoriser toutes les connexions TCP émanant d'Internet qui utilisent un port supérieur à 1024. Ce scénario présente de nombreuses opportunités pour un hacker potentiel [25].

II.2.6.2 Le filtrage de paquet avec état (Stateful) ou dynamique

Le Principe : L'amélioration par rapport au filtrage de base réside dans la maintenance des traces de session et de connexion dans les tables d'état internes du pare-feu.

Un pare-feu dynamique est un pare-feu qui maintient un "état" ou stocke des informations sur les connexions réseau actives. Lorsqu'une connexion est ouverte, le pare-feu commence à la suivre et met à jour son état interne au fur et à mesure que de nouveaux paquets sont inspectés et traités par le pare-feu. La capacité de maintenir un état permet au pare-feu d'identifier des paquets apparemment légitimes qui sortent de la séquence et ne sont pas valides. Par exemple, la plupart des organisations autorisent le trafic DNS entrant parce que les ordinateurs de l'organisation doivent effectuer des requêtes DNS pour déterminer l'adresse IP associée à divers sites web. Un pare-feu dynamique inspectant l'en-tête d'un paquet de réponses DNS entrant verra qu'il a un numéro de port de 53, qui est un numéro de port autorisé pour le trafic entrant en vertu des règles qu'il a définie.

Toutefois, un paquet de réponses DNS n'est valide que s'il répond à une requête correspondante. Un pare-feu dynamique aura un enregistrement des requêtes DNS effectuées par le système cible qui n'ont pas reçu de réponse. Si un pare-feu dynamique voit une réponse DNS sans demande correspondante, il sait qu'il doit bloquer cette réponse malveillante.

De même, pour les connexions Internet, nous autoriserons l'établissement de connexions selon les besoins, éliminant ainsi la nécessité de maintenir tous les ports supérieurs à 1024 dans un état ouvert. Pour les protocoles UDP et ICMP, il n'existe aucun mode connecté. La résolution appropriée consiste à autoriser des réponses légitimes aux paquets envoyés pendant une durée définie. Les paquets ICMP sont généralement bloqués par le pare-feu, qui est tenu de les surveiller. Néanmoins, il est jugé inutile d'obstruer les paquets ICMP de type 3 (destination inaccessible) et 4 (ralentissement de la source) qui ne sont pas utilisables par un attaquant. On peut donc choisir de les laisser passer, suite à l'échec d'une connexion TCP ou après l'envoi d'un paquet UDP.

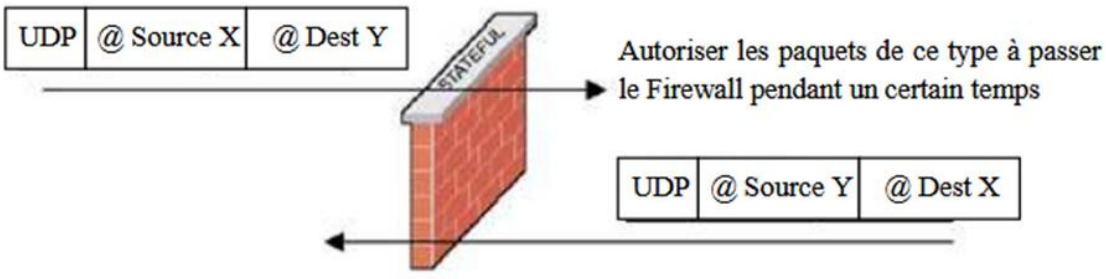


Figure 2.1 : Filtrage de paquet avec états (UDP)

Les limites : Tout d'abord, il est essentiel de s'assurer que les deux méthodologies sont exécutées efficacement par les pare-feux, étant donné que certains fabricants peuvent ne pas mettre en œuvre ces techniques de manière cohérente et précise. Par la suite, une fois que l'autorisation d'accès à un service a été accordée, il existe un manque de supervision en ce qui concerne les demandes et les réponses échangées entre les clients et les serveurs. [25].

II.2.6.3 Le filtrage applicatif (ou pare-feu de type proxy ou proxing applicatif)

Le principe : Comme l'indique sa désignation, le filtrage des applications s'effectue au niveau de la couche Application. Pour y parvenir, il est essentiel d'extraire les données du protocole de niveau 7 pour un examen approfondi. Les demandes sont gérées par des processus spécialisés ; par exemple, une requête HTTP sera filtrée par un processus proxy HTTP.. Le pare-feu rejettera toutes les requêtes qui ne sont pas conformes aux spécifications du protocole. Cela implique que le pare-feu proxy connaisse toutes les règles protocolaires des protocoles qu'il doit filtrer.

Les limites : Le principal problème qui se pose est la précision de la filtration exécutée par le proxy. La mise en place d'un mécanisme de filtrage qui ne permet à aucune donnée de traverser est extrêmement difficile, en particulier compte tenu de la multitude de protocoles de niveau 7. En outre, la nécessité de comprendre les réglementations de protocole de chaque protocole filtré crée des défis importants en termes d'adaptabilité à des protocoles nouveaux ou personnalisés. Néanmoins, il est incontestable que le filtrage de la couche application améliore la sécurité par rapport au filtrage des paquets avec état, bien qu'au détriment des performances. Cela rend la mise en œuvre d'une technologie proxy entièrement fonctionnelle impossible pour les réseaux à fort trafic de nos jours. Cependant, il est prévu que d'ici quelques années, les défis technologiques seront inévitablement relevés [25].

II.2.7 Les réactions des firewalls aux attaques classiques

II.2.7.1 IP spoofing

L'usurpation d'adresse IP implique la modification de paquets de protocole Internet (IP) afin de tromper le pare-feu en lui faisant croire qu'ils proviennent d'une adresse IP considérée comme « fiable ». Par exemple, une adresse IP associée au réseau local de l'organisation. Par conséquent, cette manipulation confère à l'acteur malveillant un accès illimité pour contourner les réglementations du pare-feu, permettant ainsi la transmission de paquets non autorisés sur le réseau de l'organisation. Les pare-feu contemporains sont capables de fournir des défenses contre de telles attaques, notamment grâce à la mise en œuvre de protocoles de réseau privé virtuel (VPN), tels que IPsec. Ce mécanisme chiffre les en-têtes des paquets, empêchant toute

personne non autorisée de les modifier ; de plus, l'intrus sera incapable de produire des paquets qui semblent provenir de ce réseau local, car l'individu ne possède pas la clé de chiffrement requise. [25].

II.2.7.2 DOS et DDOS

Les attaques par déni de service (DOS) se caractérisent par la transmission d'un nombre excessif de paquets de données à un serveur, ce qui entraîne la création d'un trafic superflu important qui bloque l'accès des utilisateurs légitimes. À l'inverse, les attaques par déni de service distribué (DDOS) sont exécutées sur plusieurs machines simultanées, ce phénomène étant souvent provoqué par un virus malveillant : le virus compromet initialement une multitude d'appareils, qui transmettent ensuite, à un moment prédéterminé, des paquets superflus ciblant une destination spécifique à partir de chaque système infecté. Cette catégorie particulière de cyberattaques est souvent qualifiée d'inondation. Dans ce contexte, les pare-feux s'avèrent largement inefficaces. En effet, les attaques DOS et DDOS utilisent généralement diverses adresses sources (l'objectif n'étant pas d'obtenir une réponse) et compliquent souvent la distinction entre ces paquets et le trafic légitime. Certains firewalls offrent une protection basique contre ce genre d'attaque, par exemple en droppant les paquets si une source devient trop gourmande, mais généralement, ces protections sont inutiles. Cette attaque brute reste un des gros problèmes actuels, car elle est très difficilement évitable [25].

II.2.7.3 Port scanning

Cette phase est en effet qualifiée de « pré-attaque » (phase de découverte). Cela implique l'identification des ports ouverts afin de déterminer les vulnérabilités présentes dans le système. Dans presque tous les cas, le pare-feu est capable d'obstruer ces analyses en désignant les ports comme « fermés ». De plus, ces activités sont facilement traçables en raison de leur origine à partir d'une source unique, qui soumet des demandes sur tous les ports de la machine. Par conséquent, il est suffisant que le pare-feu refuse temporairement l'accès à cette adresse pour empêcher tout retour d'information d'être transmis au scanner [25].

II.2.7.4 Exploit

Les exploits sont exécutés en exploitant les vulnérabilités inhérentes aux logiciels installés, tels qu'un serveur HTTP, FTP, entre autres. Le défi réside dans le fait que cette catégorie d'attaques est souvent perçue comme des requêtes totalement « légitimes », chaque attaque

présentant des caractéristiques uniques, étant donné que l'exploitation nécessite souvent la réplication de requêtes valides non prévues par le programmeur du logiciel. Autrement dit, il est quasiment impossible au firewall d'intercepter ces attaques, qui sont considérées comme des requêtes normales au système, mais exploitant un bug du serveur le plus souvent. La seule solution est la mise à jour périodique des logiciels utilisés afin de barrer cette voie d'accès au fur et à mesure qu'elles sont découvertes [25].

II.2.8 Les différents types de firewall

II.2.8.1 Les firewall bridge

Ces derniers présentent un degré de prévalence considérable. Ils fonctionnent de la même manière que les câbles réseau classiques, renforcés par une capacité de filtrage inhérente, ce qui a conduit à leur désignation de ponts. Leurs interfaces sont dépourvues d'adresse IP, ce qui facilite le transfert de paquets entre les interfaces en respectant les protocoles établis. Cette absence d'adresse IP est particulièrement avantageuse, car elle rend le pare-feu imperceptible pour l'intrus. Plus précisément, lorsqu'une requête ARP traverse le câble réseau, le pare-feu ne répond toujours pas. Ses adresses MAC ne se propagent pas au sein du réseau et, en raison de sa seule fonction de « transmission » de paquets, elle reste entièrement cachée au sein du réseau. Par conséquent, les attaques directes contre le pare-feu deviennent impossibles, car aucun paquet n'est reconnu par le pare-feu comme étant destiné à sa propre destination. Donc, la seule façon de le contourner est de passer outre ses règles de drop. Toute attaque devra donc « faire » avec ses règles, et essayer de le contourner [22]. Dans la plupart des cas, ces derniers ont une interface de configuration séparée. Un câble vient se brancher sur une troisième interface, série ou même Ethernet, et qui ne doit être utilisée que ponctuellement et dans un environnement sécurisé de préférence. Ces firewalls se trouvent typiquement sur les switches.

Avantages :

- ✓ Impossible de l'éviter (les paquets passeront par ses interfaces).
- ✓ Peu coûteux.

Inconvénients :

- ✓ Possibilité de le contourner (il suffit de passer outre ses règles).
- ✓ Configuration souvent contraignante.
- ✓ Les fonctionnalités présentes sont très basiques (filtrage sur adresse IP, port, le plus souvent en Stateless).

II.2.8.2 Les firewalls matériels

Ces types de pare-feux sont souvent intégrés directement dans des routeurs vendus par de grandes marques comme Cisco. On les appelle parfois des « boîtes noires » parce qu'ils sont profondément liés au matériel du routeur, ce qui leur permet de bien fonctionner avec le reste de l'équipement. Même si leur configuration peut être un peu compliquée, ils offrent l'avantage d'être parfaitement intégrés au système, ce qui facilite leur interaction avec les autres fonctions du routeur. Ils sont en général peu flexibles en matière de personnalisation, mais cela les rend aussi plus sûrs, car ils sont moins exposés aux attaques extérieures. Leur code est difficilement accessible, ce qui permet aux fabricants d'ajouter des mécanismes de sécurité avancés, comme des signatures numériques (ex : RSA), pour s'assurer que le logiciel n'a pas été modifié.

Ce genre de protection n'existe que sur les modèles haut de gamme, ce qui empêche l'installation de logiciels non autorisés ou de versions modifiées, renforçant ainsi la sécurité.

En plus, leur administration est souvent plus simple que celle des pare-feux de type bridge, ce que les fabricants mettent en avant comme un atout commercial. Côté sécurité, ils offrent de très bonnes garanties, sauf en cas de découverte d'une faille comme pour tout pare-feu.

Cependant, un point important à retenir : on devient complètement dépendant du constructeur pour les mises à jour. Cela peut poser problème si le fabricant tarde à réagir ou ne propose pas certaines fonctionnalités. Enfin, seuls les outils et fonctions prévus par le fabricant sont disponibles. Si on a besoin d'une fonction proposée par une autre marque, elle ne pourra pas être utilisée [22].

Avantages :

- ✓ Intégré au matériel réseau.
- ✓ Administration relativement simple.
- ✓ Bon niveau de sécurité.

Inconvénients :

- ✓ Dépendant du constructeur pour les mises à jour.
- ✓ Souvent peu flexibles.

II.2.8.3 Les firewalls logiciels

Ces pare-feux sont souvent conçus pour un usage personnel et visent à protéger un seul ordinateur, plutôt qu'un réseau complet. La plupart du temps, ce sont des solutions commerciales payantes. Elles misent généralement sur la facilité d'utilisation, ce qui les rend

accessibles au grand public. Cependant, cette simplicité peut parfois se faire au détriment de la sécurité réelle : certaines de ces solutions sont peu performantes et n'offrent qu'un niveau de protection limité. En résumé, elles sont pratiques pour les utilisateurs non experts, mais ne sont pas toujours les plus fiables pour une sécurité avancée. [22].

Avantages :

- ✓ Sécurité en bout de chaîne (le poste client).
- ✓ Personnalisable assez facilement.

Inconvénients :

- ✓ Facilement contournable.
- ✓ Leur nombre élevé complique toute tentative de comparaison.

II.3 Firewall nouvelle génération (NGFW)

Les pare-feu de nouvelle génération surpassent les modèles classiques en détectant et bloquant les logiciels malveillants avant qu'ils ne pénètrent le réseau. Grâce à leurs fonctions avancées de détection et de réponse aux menaces, les NGFW assurent une couverture sécuritaire dans les centres de données (Data center), les réseaux d'entreprise et les environnements cloud, renforçant ainsi leur position au cœur des stratégies de cybersécurité actuelles.

Les fournisseurs de NGFW offrent plusieurs types de solutions adaptées aux différents besoins des organisations, notamment des pare-feu physiques, virtuels et pour conteneurs.

- **Les pare-feu physiques** conviennent aux structures de toute taille, allant des petits et moyens campus jusqu'aux centres de données des grandes entreprises.
- **Les pare-feu virtuels** sont destinés aux environnements cloud comme AWS, Azure, Google Cloud Platform, IBM Cloud, Oracle Cloud ou les clouds privés, en fournissant la souplesse requise pour les opérations cloud.
- **Les pare-feu pour conteneurs** visent les applications s'exécutant dans des environnements conteneurisés, offrant une meilleure visibilité et sécurité pendant l'exécution, notamment dans les petits déploiements et les composants d'infrastructure compatibles avec Docker.

Peu importe l'architecture, une solution NGFW est disponible pour s'adapter à tous les besoins en sécurité. Lors de l'évaluation des solutions NGFW, certains critères essentiels doivent être pris en compte :

- Performances
- Intégrations de sécurité tierces

- Facilité d'utilisation
- Efficacité du blocage des menaces
- Les modèles de tarification et de consommation
- Fonctionnalités supplémentaires telles que la visibilité des applications, la sécurité du cloud hybride et la gestion centralisée.

II.3.1 Meilleurs fournisseurs de NGFW pour 2025

II.3.1.1 Palo Alto Networks

Palo Alto Networks maintient sa position dominante sur le marché des pare-feu de nouvelle génération, étant classé comme Leader dans le rapport Enterprise Firewalls Wave™ de Forrester pour le quatrième trimestre 2024. Le fait que Palo Alto occupe cette place de leader depuis dix ans témoigne de la régularité de son innovation et de sa fiabilité.

La gamme NGFW de l'entreprise comprend des pare-feu physiques (série PA), virtuels (série VM) et pour conteneurs (série CN). Tous reposent sur une architecture à passage unique, qui analyse le trafic, qu'il s'agisse d'applications, de menaces ou de contenu, tout en l'associant à l'utilisateur, peu importe son appareil ou sa localisation. Grâce à l'intégration d'un moteur d'identité cloud et à la prise en charge de la sécurité SaaS via CASB, Palo Alto propose une protection adaptée aux environnements hybrides et multi-cloud.

L'entreprise renforce sa technologie avec de l'intelligence artificielle avancée et du machine learning, assurant une défense en temps réel contre les ransomwares et les menaces zero-day. Elle propose également des solutions pour la sécurité IoT et OT, intégrant des fonctionnalités comme la micro-segmentation, l'analyse comportementale et la visibilité sur les appareils. Ces éléments confirment la position stratégique de Palo Alto pour les organisations qui mettent en œuvre des approches Zero Trust et cloud hybride. [26]

PA-5440 Series **PA-7000 Series** **PA-5450 Series**

Figure 2.2 : Séries de Firewall de Palo Alto Networks

II.3.1.2 Fortinet: FortiGate

Les pare-feux de nouvelle génération FortiGate (NGFW) de Fortinet sont reconnus pour leur haute performance et leurs fonctionnalités de sécurité étendues. Basés sur un système d'exploitation unifié, ils assurent une protection homogène dans les environnements physiques, virtuels et cloud, en sécurisant efficacement tous les points d'entrée du réseau, quelle que soit leur taille. Ils offrent des fonctions avancées comme la prévention des intrusions, le contrôle des applications et la protection contre les logiciels malveillants, assurant une sécurité complète à travers une seule plateforme.

Les pare-feu FortiGate offrent une large gamme de modèles pour répondre aux besoins de diverses organisations, allant des petites entreprises aux grands centres de données. Les séries populaires incluent les FortiGate 30G, 50G, 70G, 100G, ainsi que les modèles virtuels pour les environnements cloud. Voici quelques exemples et leurs cas d'utilisation :

Séries FortiGate pour entreprises:

- **FortiGate 30G, 50G, 70G:**

Ces modèles sont conçus pour les petites et moyennes entreprises, offrant une protection NGFW avec des performances optimisées pour le traitement des menaces et l'inspection IPS.

- **Séries FortiGate pour les grands réseaux:**

Les modèles de la série 1000 et supérieurs sont adaptés aux grands réseaux d'entreprises, aux centres de données et aux environnements de campus, offrant des performances élevées et des fonctionnalités avancées pour la sécurité et la mise en réseau.

- **FortiGate Virtual:**

Les versions virtuelles des pare-feu FortiGate permettent une intégration transparente aux environnements cloud publics et privés, offrant la même sécurité que les modèles physiques.

A titre d'exemple, en 2024, Fortinet a introduit la série FortiGate 200G, spécialement développée pour renforcer la sécurité des réseaux de campus. Équipée du processeur de sécurité de cinquième génération (SP5), cette série fournit un débit de pare-feu amélioré, une détection des menaces alimentée par l'AI, ainsi que des ports 5GE compatibles avec la dernière norme Wi-Fi 7. Ces caractéristiques permettent aux entreprises de mieux gérer et sécuriser un volume croissant de trafic riche en données et d'applications cloud [26].

Figure 2.3 : Firewall FortiGate de la série 200G

a) Facteurs de différenciation concurrentielle des pare-feu FortiGate

- **Convergence des réseaux et de la sécurité**

L'approche de Fortinet en matière de réseau sécurisé (Fortinet Secure Networking) combine les fonctions réseau et sécurité sur une seule et même plateforme. Cette intégration élimine la dépendance à des solutions ponctuelles et renforce la protection des environnements dynamiques contre des menaces avancées, grâce à l'intelligence artificielle. Elle contribue également à une meilleure productivité et à une expérience utilisateur optimisée.

- **SD-WAN intégré et périphérie Zero Trust**

FortiGate regroupe les fonctionnalités SD-WAN et Zero Trust Edge dans une solution unifiée, conçue pour sécuriser les bords en constante expansion du réseau. En associant un SD-WAN avancé à une solution SASE complète, Fortinet garantit une sécurité renforcée pour les environnements hybrides.

FortiOS propose des fonctionnalités comme le SD-WAN, le CASB (courtier d'accès aux services cloud), le ZTNA (accès réseau Zero Trust), et la passerelle web sécurisée. Grâce à ses modes de déploiement flexibles, la solution facilite l'administration, réduit les coûts et assure un excellent retour sur investissement.

- **Capacités de déchiffrement du trafic**

Étant donné que la majorité du trafic internet est désormais chiffrée, les menaces de sécurité se sont accrues. Fortinet offre des capacités de déchiffrement TLS qui assurent la sécurité des environnements hybrides et protègent les données sensibles sur l'ensemble du réseau. Ces solutions permettent d'intercepter et de décoder le trafic chiffré, ce qui rend possible l'identification et la neutralisation de menaces qui passeraient autrement inaperçues.

- **Filtrage DNS**

Le service de filtrage DNS FortiGuard est directement intégré aux pare-feu FortiGate NGFW. Il repose sur l'intelligence artificielle, le machine learning et le partage de renseignements sur les menaces pour contrer les menaces basées sur le DNS.

Parmi ses fonctionnalités clés, nous avons :

- ✓ Fonctionnalité de serveur DNS polyvalente compatible avec IPv4 et IPv6.
- ✓ Analyse quotidienne de milliards de domaines, alimentée par l'IA et le machine Learning.
- ✓ Catégorisation DNS en plus de 90 groupes pour un contrôle granulair.
- ✓ Protection complète avec recherche sécurisée et détection d'algorithmes de génération de domaines (DGA) [27].

II.3.1.3 Juniper Networks

La série SRX représente la gamme de pare-feu nouvelle génération (NGFW) de Juniper Networks, proposée sous plusieurs formats : équipements physiques (SRX), versions virtuelles (vSRX) et solutions en conteneurs (cSRX). La version vSRX peut être déployée sur l'hyperviseur du client ou dans les environnements cloud tels qu'AWS, Microsoft Azure, Google Cloud Platform et Oracle Cloud Infrastructure. Les NGFW de la série SRX offrent une sécurité performante avec des services intégrés pour protéger les applications, prévenir les intrusions et détecter les menaces avancées, adaptés à tous types d'organisations.

Les pare-feu NGFW de Juniper se distinguent par leur haut niveau d'efficacité, atteignant un taux de blocage des exploits de 99,7 % sans aucun faux positif, selon le rapport 2024 de CyberRatings.org consacré aux pare-feu réseau dans le cloud.

En 2024, Juniper Networks a enrichi sa série SRX avec les modèles SRX4300 et SRX4700, destinés respectivement aux entreprises de taille intermédiaire et aux infrastructures à grande échelle. Le SRX4300 convient aux campus et aux bureaux régionaux, en fournissant une sécurité robuste et une prévention avancée des menaces. Le SRX4700, quant à lui, est destiné à des environnements plus complexes, tels que les centres de données, en protégeant efficacement les réseaux centraux et périphériques. Ces deux modèles intègrent la prévention prédictive des menaces alimentée par l'IA, des capacités « zero trust » et une intégration fluide avec les architectures réseau actuelles, illustrant l'engagement de Juniper à proposer des solutions de sécurité flexibles et évolutives [26].

a) Les solutions de Juniper Networks

- **Pare-feux SRX**

Ces pare-feu nouvelle génération de Juniper, disponibles en formats physique, virtuel et conteneurisé, assurent la protection du périmètre réseau, des centres de données et des applications cloud.

- **vSRX Virtual Firewall**

Conçu pour offrir une sécurité performante, le vSRX protège efficacement les environnements cloud, qu'ils soient privés, publics ou hybrides.

- **Pare-feu de conteneur cSRX**

Le cSRX, hautement flexible, fournit des services de sécurité avancés pour renforcer la visibilité et la protection des applications déployées dans des environnements de conteneurs et de micro services.

Le SRX5600 est idéal pour sécuriser les centres de données des grandes entreprises, les infrastructures des fournisseurs de services et les réseaux du secteur public.
Performances pare-feu (max.) : 1,44 Tbit/s
Performances IPS : 245 Gbit/s
Performances VPN : 269 Gbit/s
Nombre maximal de sessions simultanées : 182 millions

Figure 2.4 : Firewall SRX5600 de Juniper Networks

II.3.1.4 Cisco Secure Firewall

Le pare-feu nouvelle génération Cisco Secure Firewall propose une protection renforcée contre les menaces, une visibilité accrue sur les applications et une gestion centralisée des politiques de sécurité. Il fournit une défense homogène dans les environnements physiques, virtuels et cloud, assurant une couverture constante et une gestion simplifiée.

Classé parmi les leaders dans The Forrester Wave™ : Enterprise Firewall Solutions Q4 2024, il intègre des fonctions avancées basées sur l'intelligence artificielle et le machine learning, permettant une adaptation aux besoins des entreprises actuelles. Grâce à ces technologies, la solution automatise la gestion des politiques de sécurité et offre une visibilité sur le trafic chiffré, permettant une protection proactive face aux nouvelles menaces. L'inspection multicouche, reposant notamment sur le moteur SnortML, assure une prévention efficace des intrusions, ce qui renforce la sécurité globale dans des architectures réseau variées. Ces atouts font de Cisco un fournisseur fiable pour les organisations en quête de pare-feux adaptatifs et évolutifs.

a) Les solutions de Cisco Secure Firewall

- **Secure Firewall 3100 Series**

Destinée aux entreprises de taille moyenne à grande souhaitant renforcer le télétravail, cette série assure des performances VPN optimales. Elle utilise l'apprentissage automatique pour identifier de manière passive les applications et les menaces dans le trafic chiffré, sans avoir besoin de déchiffrer les données.

- **Firepower 2100 series**

Conçue pour les grandes entreprises et leurs succursales, cette série permet de choisir la méthode de gestion la mieux adaptée à l'environnement et aux processus de l'organisation.

- **Firepower 4100 series**

Idéale pour les grands campus et les centres de données, elle offre des pare-feux logiques, une surveillance du trafic chiffré, une protection contre les attaques DDoS, le regroupement de dispositifs pour de meilleures performances, la haute disponibilité, la création de VPN évolutifs et la détection des intrusions réseau.

- **Firepower 9300 series**

Pensée pour les opérateurs télécoms et les data centers à haute performance, cette plateforme modulaire permet la mise en place de pare-feux logiques indépendants, des VPN extensibles, une surveillance du trafic web chiffré, une protection contre les DDoS, ainsi qu'une gestion optimisée des performances et de la disponibilité.

- **ASA 5500-X**

Ces appliances associent un matériel solide à des technologies avancées d'inspection pour offrir aux PME et aux succursales une protection fiable contre les menaces les plus récentes.

Figure 2.5 : Firewall Cisco Secure ASA 5500

II.3.1.5 Forcepoint

L'offre de sécurité réseau de Forcepoint comprend sept séries de pare-feu différentes, avec des objectifs différents. Toutes les séries comprennent une gestion centralisée, et une sécurité étendue telle que VPN, IPS, inspection cryptée, SD-WAN et proxies d'applications critiques. Selon Forcepoint, son NGFW est conçu pour réduire la complexité et le temps nécessaire pour faire fonctionner un réseau de manière fluide et sécurisée. Le Forcepoint Next-Gen Firewall est construit autour d'un noyau logiciel unifié qui offre des capacités cohérentes, une accélération et une gestion centralisée dans tous les types de déploiements. Leur centre de

gestion de la sécurité (SMC) peut configurer, surveiller et mettre à jour jusqu'à 2000 appliances Forcepoint NGFW physiques, virtuelles et cloud [26].

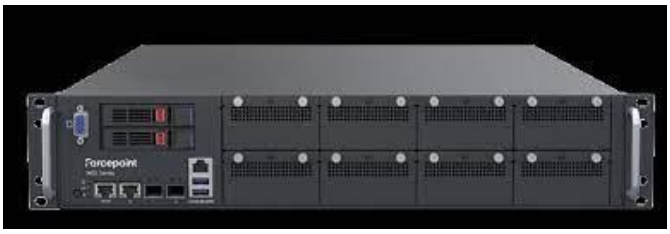


Figure 2.6 : Firewall Forcepoint 3400 series

II.4 Conclusion

À l'ère du numérique, où les cybermenaces évoluent rapidement en complexité et en fréquence, les pare-feu de nouvelle génération (NGFW) s'imposent comme une réponse indispensable aux limites des pare-feu traditionnels. Contrairement à ces derniers, les NGFW intègrent des fonctions de sécurité avancées, telles que l'inspection approfondie du trafic, la détection et la prévention des intrusions, la visibilité applicative et l'analyse des menaces en temps réel, souvent renforcées par l'intelligence artificielle et le machine learning.

À travers ce chapitre, nous avons mis en évidence les capacités différenciatrices de plusieurs fournisseurs majeurs, dont Palo Alto Networks, FortiGate, Juniper Networks, Cisco et Forcepoint. Chacun propose des solutions adaptées aux environnements physiques, virtuels et cloud, répondant aux besoins de sécurité des entreprises modernes. De la convergence réseau-sécurité aux fonctionnalités de Zero Trust, en passant par le déchiffrement du trafic chiffré et le filtrage DNS intelligent, les NGFW incarnent une protection globale et proactive.

Ainsi, les NGFW ne se contentent plus de bloquer les menaces connues : ils anticipent, détectent et neutralisent les attaques sophistiquées, tout en simplifiant la gestion de la sécurité à grande échelle. Leur adoption constitue aujourd'hui un pilier central des stratégies de cybersécurité, en particulier dans les environnements hybrides et distribués.

Chapitre 3

Méthodologie de test: Emulation avec Eve-ng – Installation et Configuration

3

Méthodologie de test: Emulation avec Eve-ng Installation et Configuration

III.1 Introduction

Ce chapitre expose les différentes étapes pour mettre en œuvre l'environnement de test adapte au contexte de notre projet. La plate-forme en question sert à émuler un réseau virtuel afin de permettre l'intégration, la configuration et le test de scenarios de sécurité basée sur un pare-feu nouvelle génération Fortigate. Nous avons commencé par l'installation de l'outil de virtualisation VMware Workstation, avec lequel nous avons créé et géré les machines virtualisées entre-autre EVE-NG, pour Emulated Virtual Environment – Next Génération, un environnement de simulation dédié de réseau.

Ensuite, nous avons intégré à cette plateforme les diverses images virtuelles des équipements utilisés pour nos tests. Pour le transfert entre notre machine locale et EVE-NG, nous avions recours à FileZilla/WinSCP en utilisant le protocole SFTP.

Enfin, nous avons téléchargé du site officiel du Fortinet l'image du pare-feu FortiGate, et l'incorporé à notre cadre de virtualisation. C'était la première phase sur laquelle nous avons bâti nos paramétrages et expérimentations des solutions de sécurité choisies pour les tests.

III.2 VMware Workstation

VMware est une entreprise technologique américaine créée en 1998, qui fonctionne en tant que filiale d'EMC Corporation depuis 2004, puis rachetée par Dell en 2016. Elle fournit une gamme de produits propriétaires associés à la virtualisation des architectures x86. De plus, le terme est utilisé pour désigner une suite de logiciels de virtualisation [28].

VMware Workstation constitue un instrument de virtualisation des ordinateurs de bureau développé par VMware, qui facilite la mise en place d'un environnement de test à des fins de développement logiciel ou d'évaluation de l'architecture complexe d'un système d'exploitation avant son installation effective sur une machine tangible [28].

III.2.1 Téléchargement et installation de VMware Workstation

Nous avons téléchargé VMware Workstation version pour Windows du site officiel de VMware [28]. Les étapes d'installation sont résumées dans les captures suivantes :

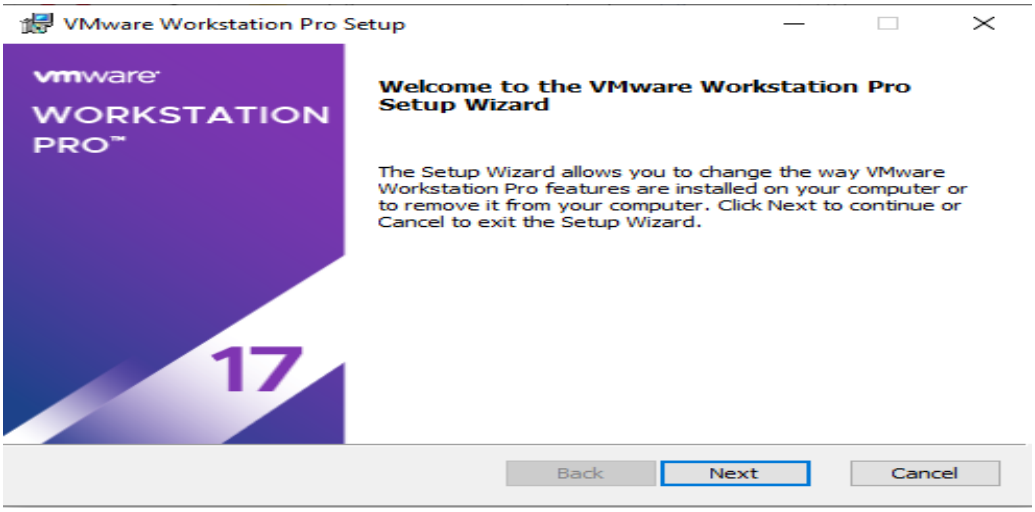


Figure 3.1: Installation de VMware Workstation pro 17

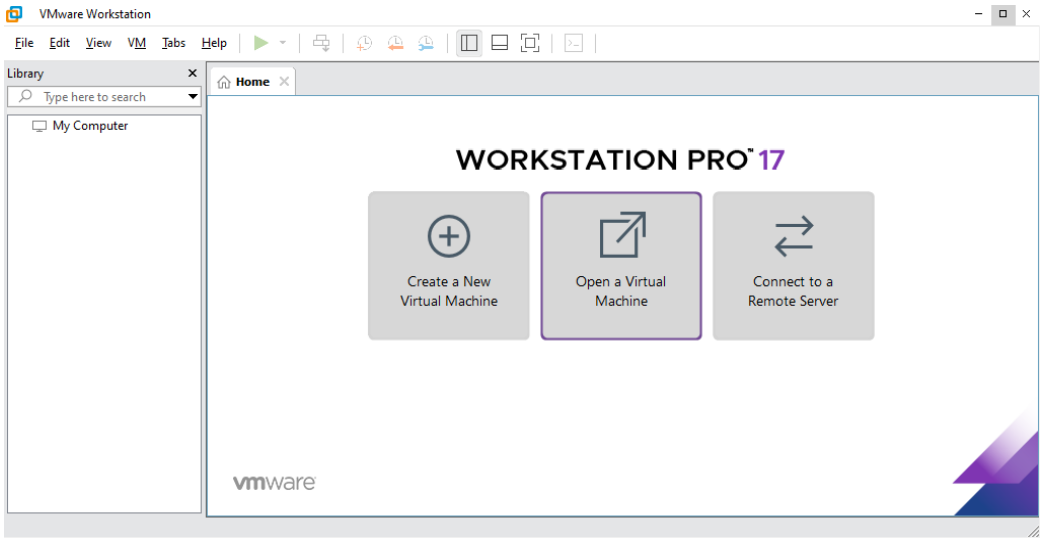


Figure 3.2: Interface de VMware Workstation pro 17

III.3 Plateforme EVE-NG

EVE-NG est une plateforme d'émulation réseau avancée permettant de concevoir des topologies complexes en simulant divers équipements tels que routeurs, commutateurs, pare-feu etc, dans un environnement entièrement virtualisé. Elle se distingue par sa grande flexibilité et sa compatibilité avec un vaste éventail de systèmes d'exploitation réseau, notamment Cisco IOS, Juniper JunOS, Huawei VRP, Fortinet entre autres.

EVE-NG prend en charge plusieurs technologies de virtualisation, notamment la virtualisation basée sur des conteneurs (Docker), la virtualisation basée sur des machines virtuelles (VMware, KVM) et la virtualisation basée sur des émulations matérielles (QEMU). Cette polyvalence permet aux utilisateurs de choisir la méthode de virtualisation qui convient le mieux à leurs besoins et à leur infrastructure existante. En voici quelques caractéristiques :

- Interface web HTML5 (aucun logiciel client requis)
- Support de plusieurs systèmes : Cisco IOS, JunOS, VRP, pfSense, etc.
- Compatible avec QEMU, Docker, IOL, Dynamips
- Utilisée pour la formation, la certification (CCNA, CCNP, etc.), les tests réseau et la cybersécurité
- Disponible en version gratuite (Community) et payante (Pro/Enterprise)

Enfin, EVE-NG offre une interface utilisateur graphique conviviale qui permet de créer et de gérer facilement des topologies réseau. Nous pouvons glisser-déposer des appareils réseau virtuels sur une toile virtuelle, connecter les appareils à l'aide de câbles virtuels et configurer les paramètres réseau à l'aide d'une interface claire et intuitive.

III.3.1 Téléchargement et Importation de la plateforme EVE-NG

Nous avons téléchargé EVE-NG Community version OVA (Open Virtual Appliance-VM complète dans un seul fichier-) [29], [30] et l'importé dans VMware Workstation afin de l'utiliser pour nos travaux et tests, en voici les étapes :

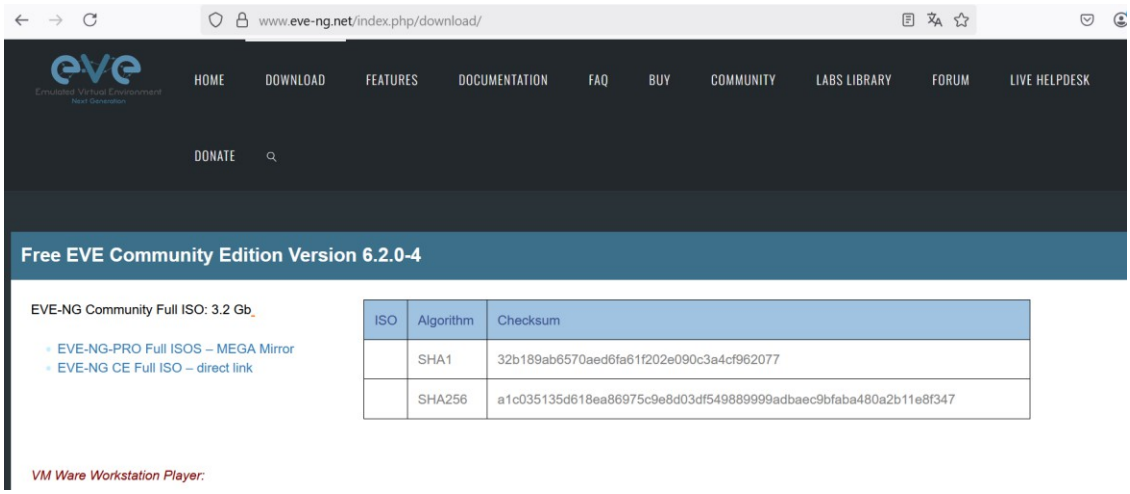


Figure 3.3: Site de téléchargement eve-ng.net

Seule la version .iso est disponible sur le site officiel [29]. Pour des raisons de facilité, nous avons opté pour la version .ova, disponible sur le site [30]. (Figure 3.4).

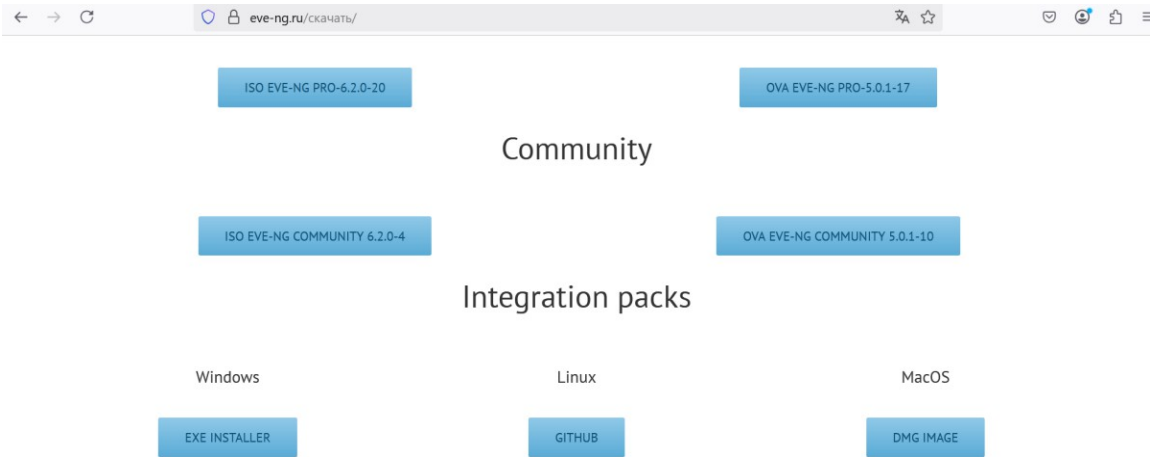


Figure 3.4: Site de téléchargement d'eve-ng version .ova

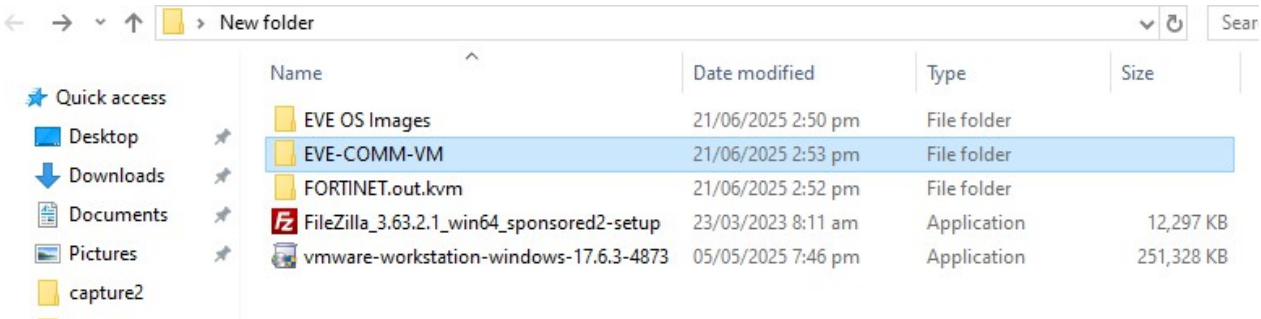


Figure 3.5: Téléchargement d'EVE-COMM-VM

Pour l'importation, voici les captures :

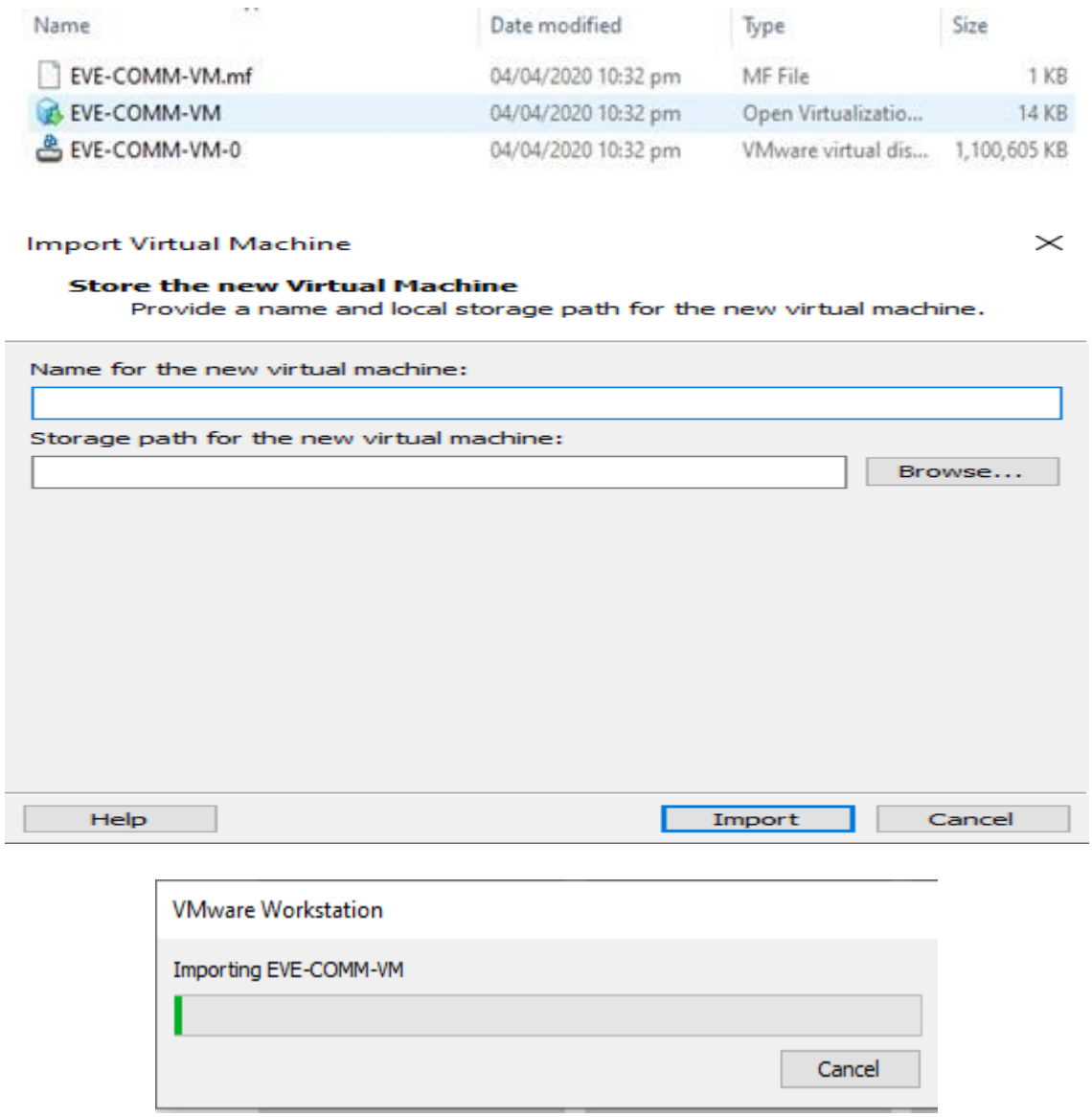


Figure 3.6: Importation d'EVE-COMM-VM

Une fois importée, la machine virtuelle ***EVE-COMM-VM*** est prête pour l'utilisation. (Figure 3.7).

Nous cliquons sur le bouton "**Power on this virtual machine**". La machine démarre en mode CLI (figure 3.8), nous indiquant son adresse IP qui nous permet d'accéder à l'interface graphique d'EVE-NG.

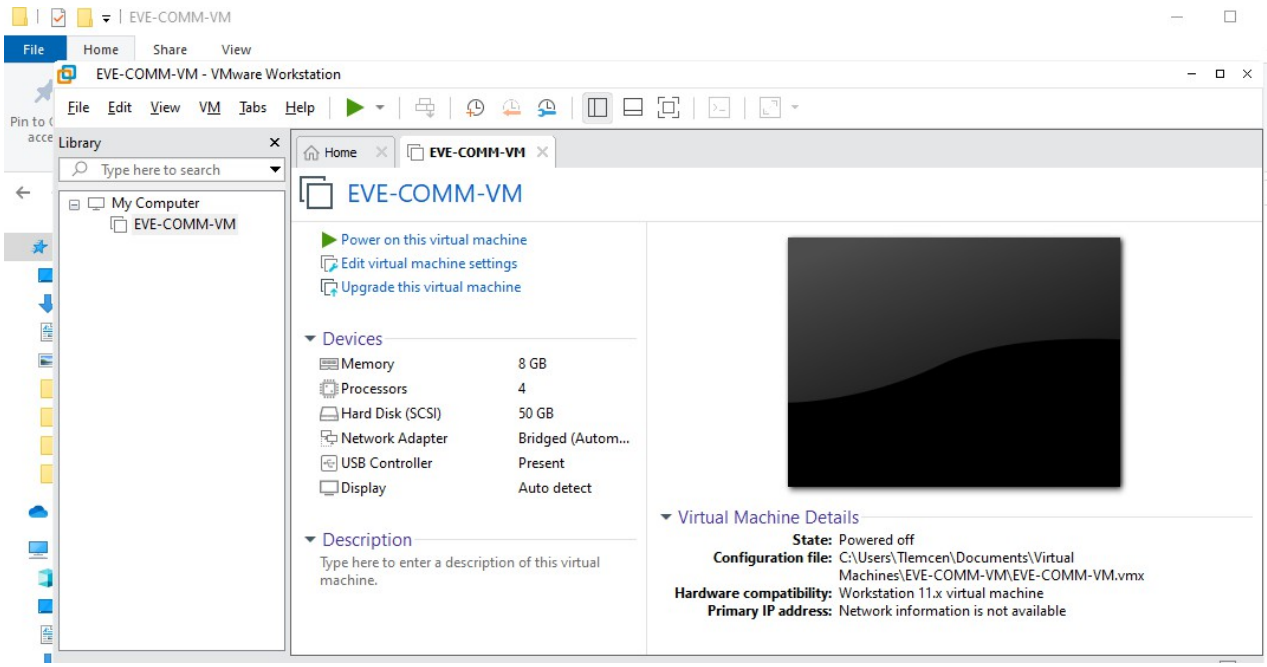


Figure 3.7: Amorçage d'EVE-COMM-VM

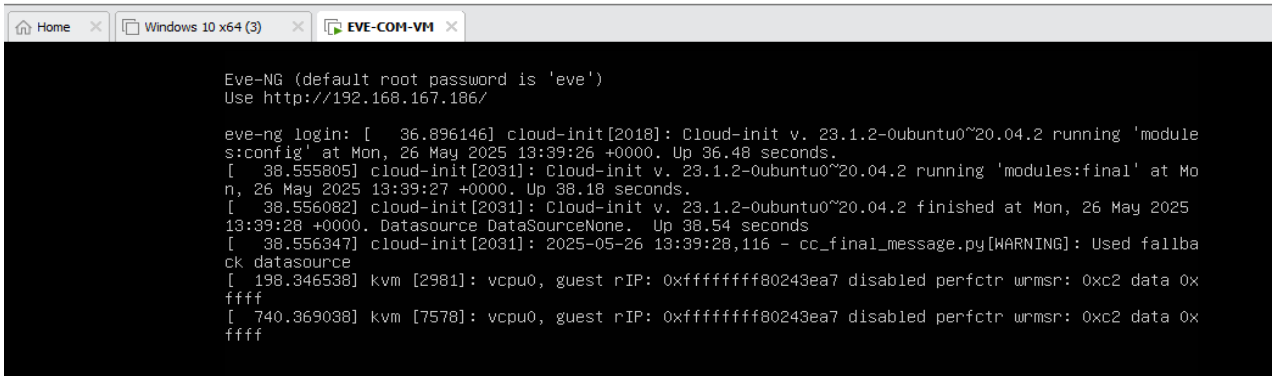


Figure 3.8: Interface CLI d'EVE-NG

On note l'adresse IP : **192.168.167.186**

Pour accéder à l'interface graphique d'eve-ng, on utilise n'importe quel navigateur en saisissant l'adresse IP 192.168.167.186 :

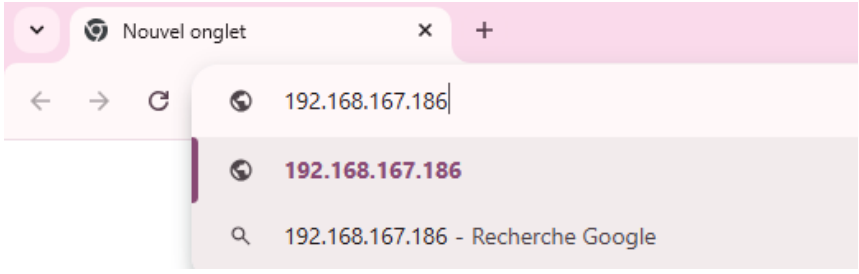


Figure 3.9: EVE-NG via interface Web

On renseigne ensuite les champs d'authentification comme suit :

Username : admin

Password : eve

Native console : Htlm5 console

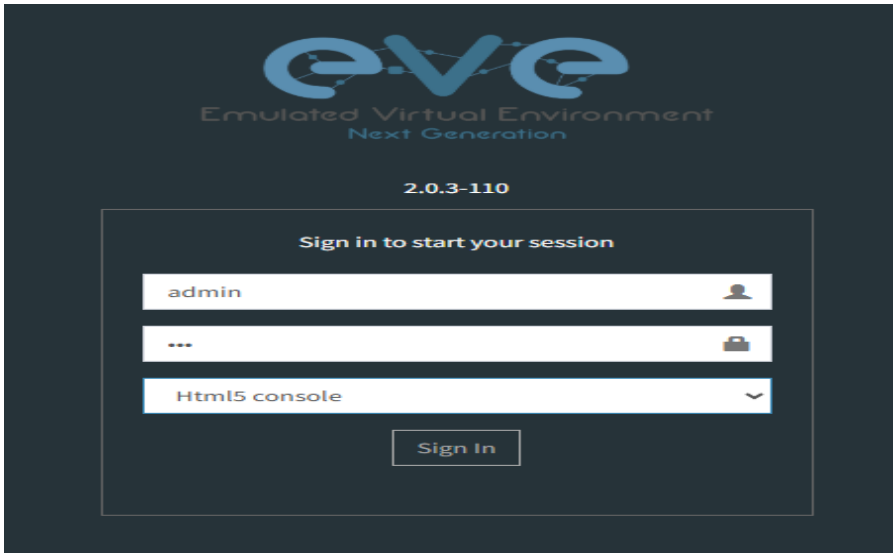


Figure 3.10: Interface d'accès à EVE-NG

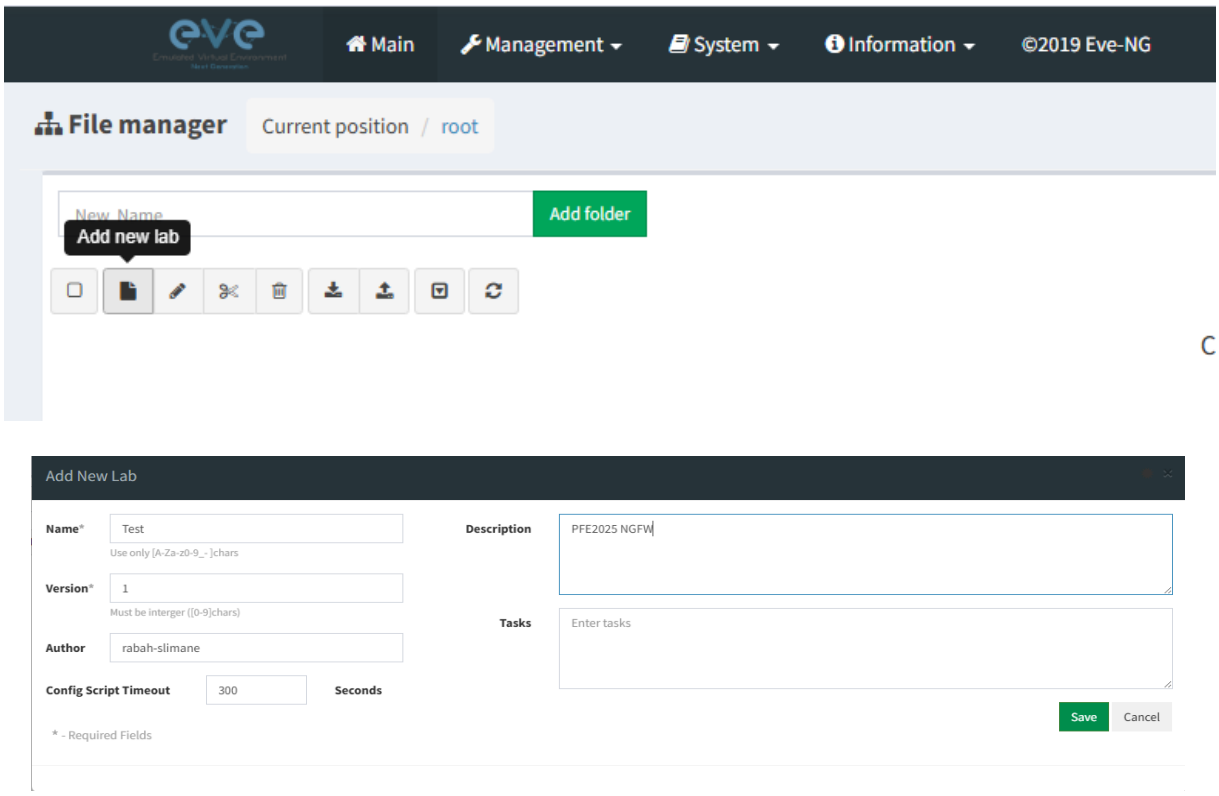


Figure 3.11: Création d'un nouveau lab sous EVE-NG

Pour pouvoir utiliser des équipements réseau tels que des routeurs, switchs, etc, il va falloir ajouter des images des équipements réseau souhaités dans l'environnement EVE-NG.(Figure 3.11).

Ces images peuvent être téléchargées à partir de sources officielles ou communautaires. Pour notre part, nous avons pu télécharger un dossier nomme « EVE OS Images » contenant les images les plus utilisées.

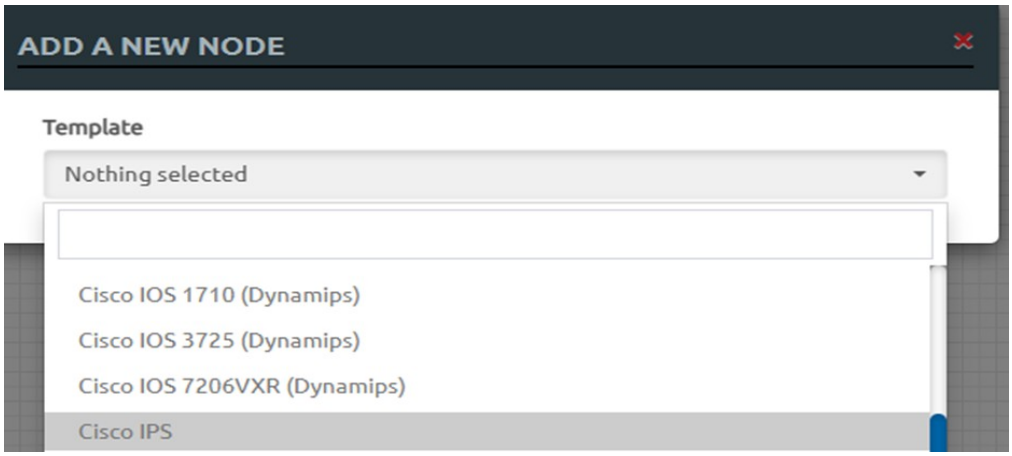


Figure 3.12: Absence des équipements sous EVE-NG

Pour cela, nous avons fait appel à un utilitaire de transfert de fichiers tels que FileZilla ou WinSCP.

III.4 FileZila

FileZilla constitue un client FTP (File Transfer Protocol) qui facilite le chargement et le téléchargement de fichiers sur un serveur distant, comprenant les composants d'un site Web d'un fournisseur de services d'hébergement. Il représente une solution open source librement accessible et est disponible en langue française.

FireZilla est largement considéré comme le client FTP par excellence, offrant une multitude de fonctionnalités :

- ✓ prise en charge de FTP, FTPS (utilisant SSL/TLS) et SFTP (protocole de transfert de fichiers SSH),
- ✓ compatibilité avec IPv4 et IPv6,
- ✓ la possibilité de transférer des fichiers volumineux (supérieurs à 4 Go),
- ✓ la possibilité de reprendre les téléchargements et les chargements interrompus,
- ✓ la possibilité de configurer les limites de vitesse de transfert pour réguler l'utilisation de la bande passante, capacités de reconnexion rapide,
- ✓ la synchronisation d'un répertoire local avec un répertoire distant [29].

III.4.1 Téléchargement et installation de FileZila

L'outil FileZila est téléchargé à partir du site officiel [30], figure 3.13.

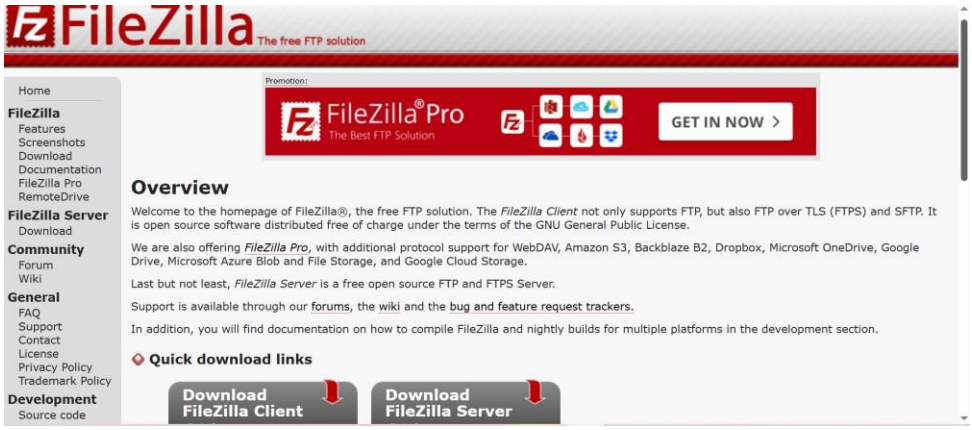
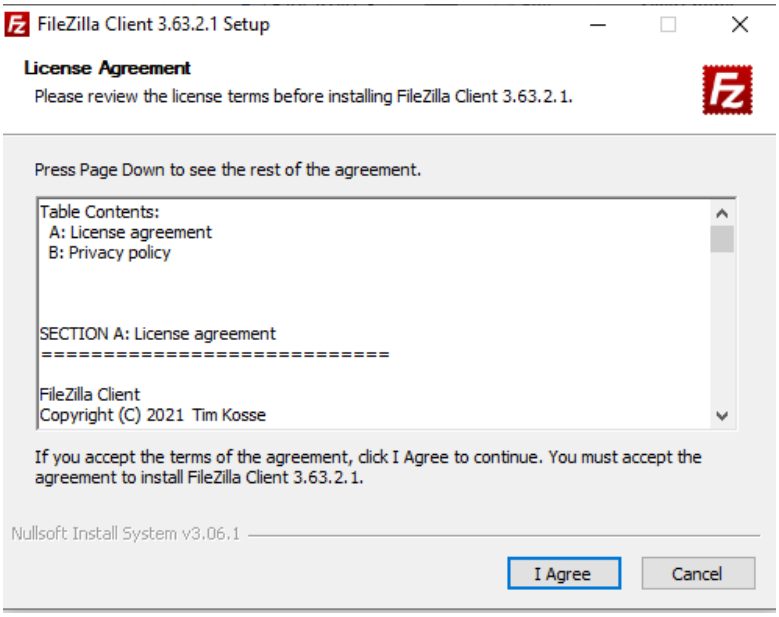


Figure 3.13: Site de téléchargement de FileZila

L'installation se fait en quelques clics.



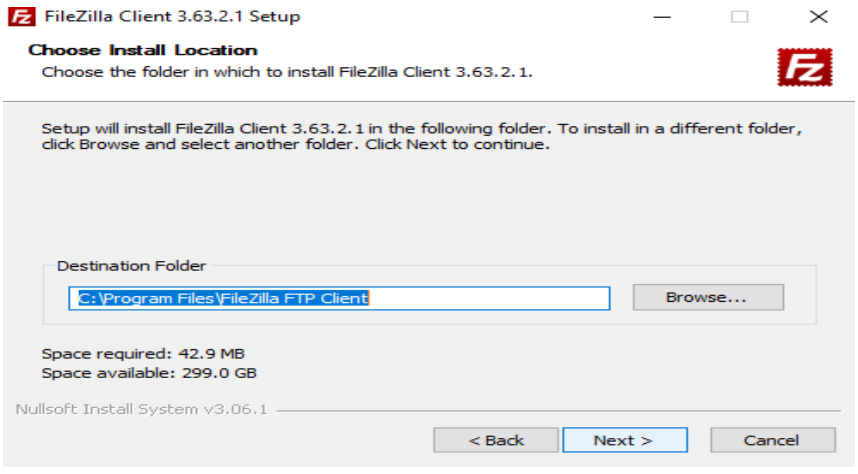


Figure 3.14: Installation de FileZila

III.4.2 Transfert des images des équipements sur Eve-ng

Pour ouvrir une session SFTP (SSH File Transfer Protocol) vers EVE-NG depuis notre host, on lance le client FileZila, et on renseigne les paramètres de connexion :

Hôte (Host) : 192.168.167.186

Nom d'utilisateur (Username) : root

Mot de passe (Password) : eve

Port : 22 (SFTP)

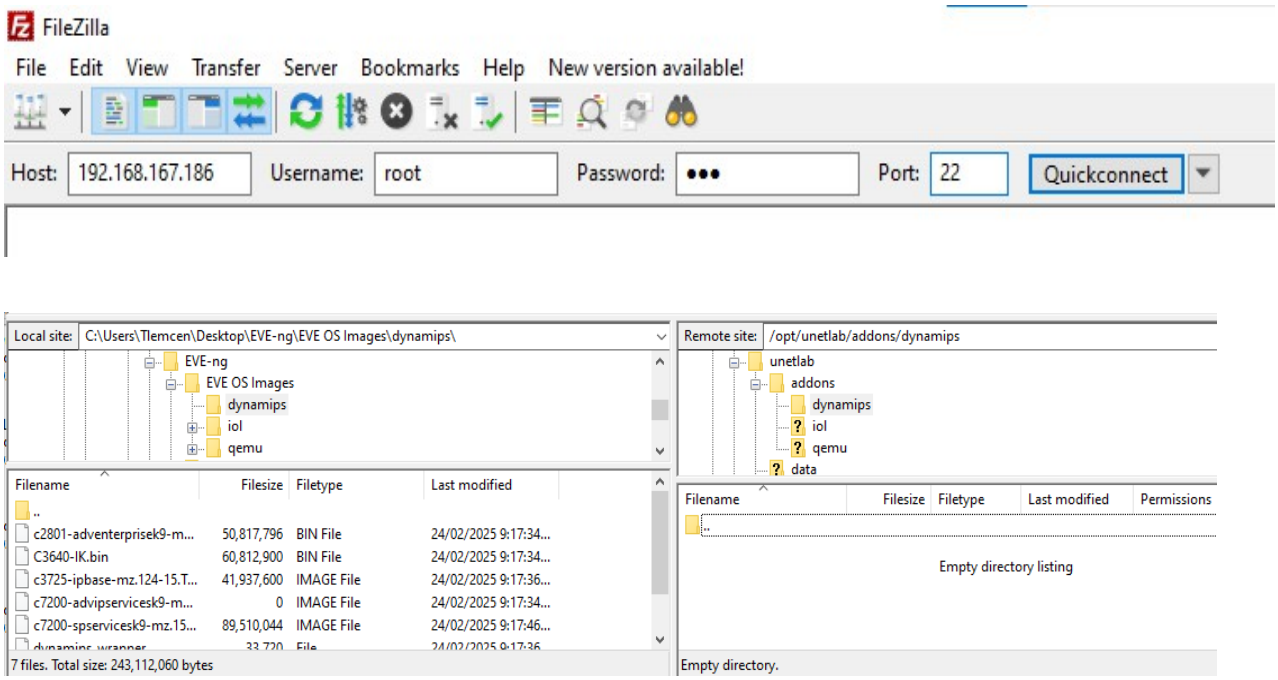


Figure 3.15: Ouverture d'une session SFTP vers EVE-NG

Pour transférer les images des équipements réseau, on ouvre le dossier « EVE OS Images » qui contient ces images sur notre hôte local, puis on va sur « Remote site » en tape (/opt/unetlab/addons/) et on fait transférer les fichiers. On fait cela pour les 3 répertoires dynamics, iol et qemu.

Après le transfert, on voit apparaitre les équipements sur l'interface Eve-ng (figure 3.16).

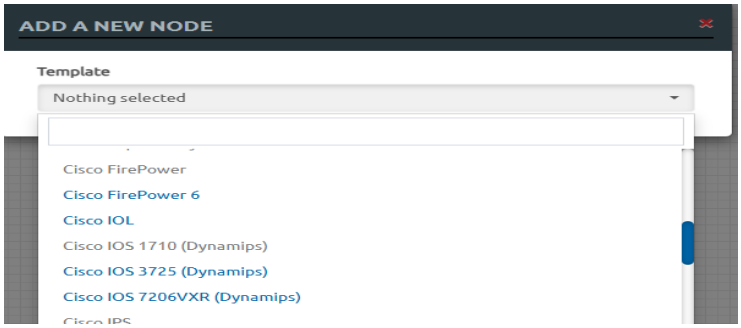


Figure 3.16: Visibilité des équipements réseau sur Eve-ng

III.5 Téléchargement et Intégration du Firewall Fortigate sur Eve-ng

Nous pouvons voir sur la figure suivante, le manque du firewall fortigate sur la plateforme EVE-NG, donc il faudra importer son image comme nous venons de le faire dans la section précédente.

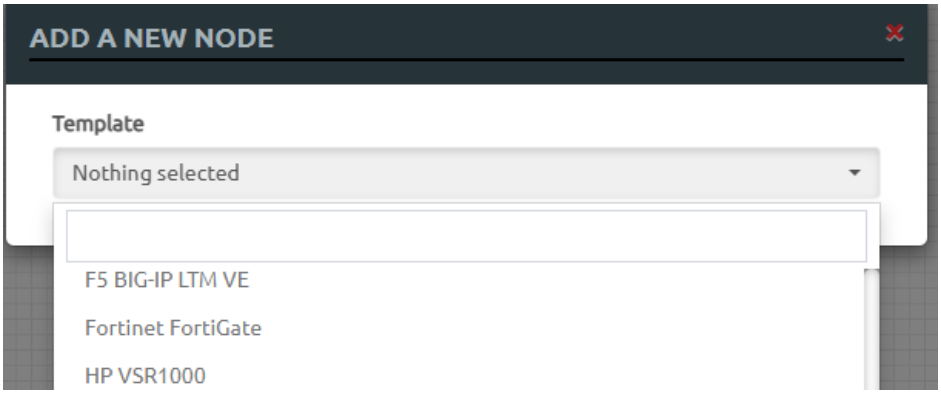


Figure 3.17: Absence du firewall Fortgate sur Eve-ng

III.5.1 Téléchargement du Firewall Fortigate

Le téléchargement passe d'abord par la création d'un compte et la connexion avec ce compte au site officiel fortinet.

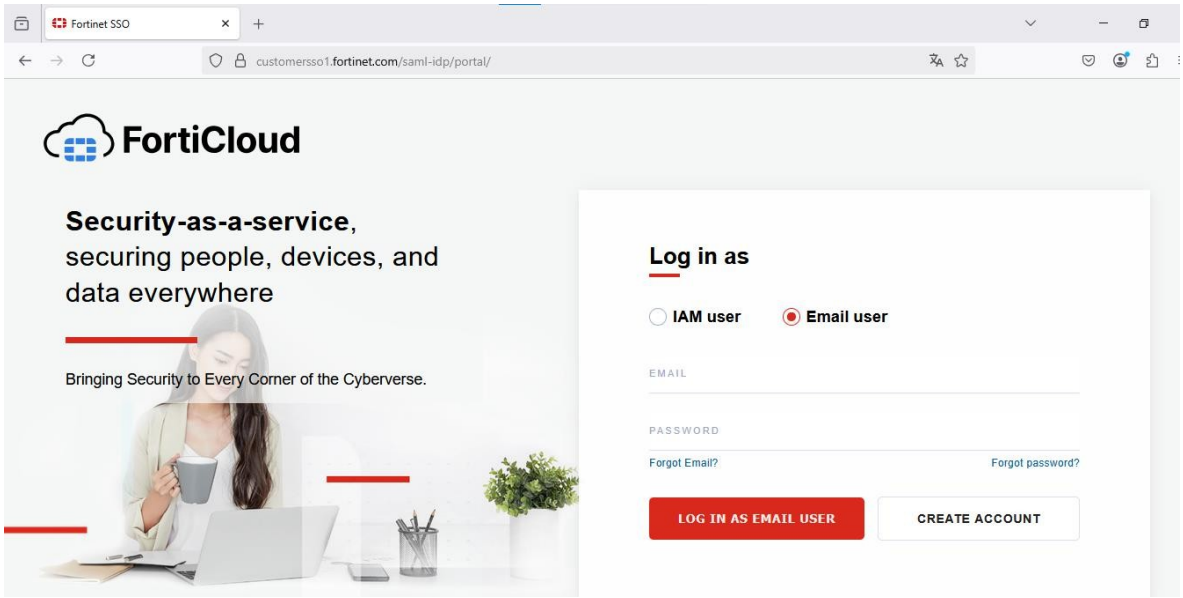


Figure 3.18: Connexion au site de fortinet

Une fois connecté, nous pourrons accéder au tableau de bord. Nous cliquerons sur "VM Images", nous choisissons le produit Fortigate et la plateforme KVM, et nous procédons au téléchargement de la version : 7.2.11

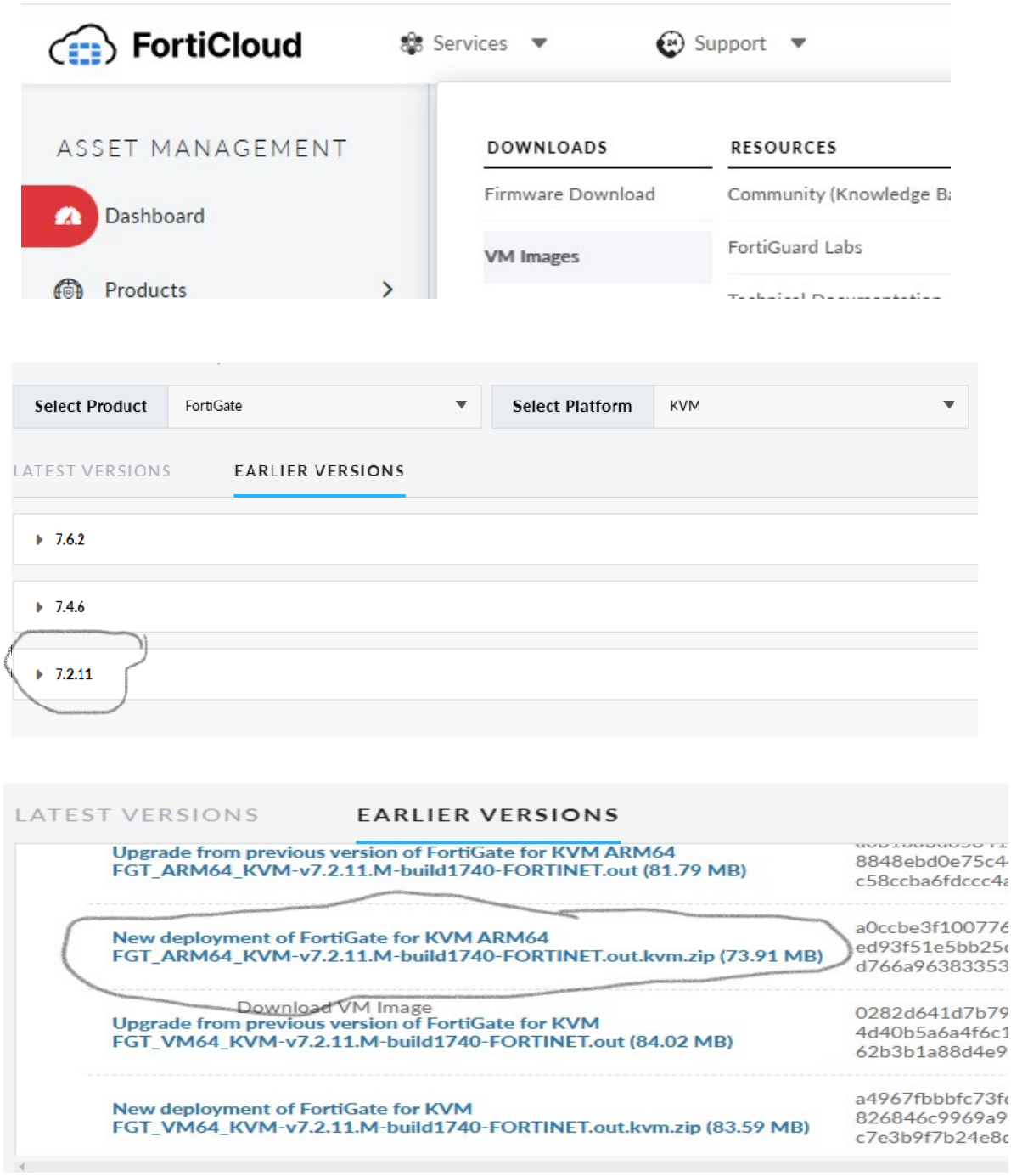


Figure 3.19: Téléchargement du Firewall Fortigate-7.2.11 du site de fortinet

III.5.2 Intégration du Firewall Fortigate sur Eve-ng

Tout d'abord, nous ouvrons le dossier qemu sur (Remote Site=Eve-ng), puis nous créons un nouveau répertoire qui sera nommé fortinet-FGT-7.2.11. Ensuite, dans le panneau « Site local » (Local Site), nous accédons au dossier FortiGate, et nous transférons-le vers Eve-ng.

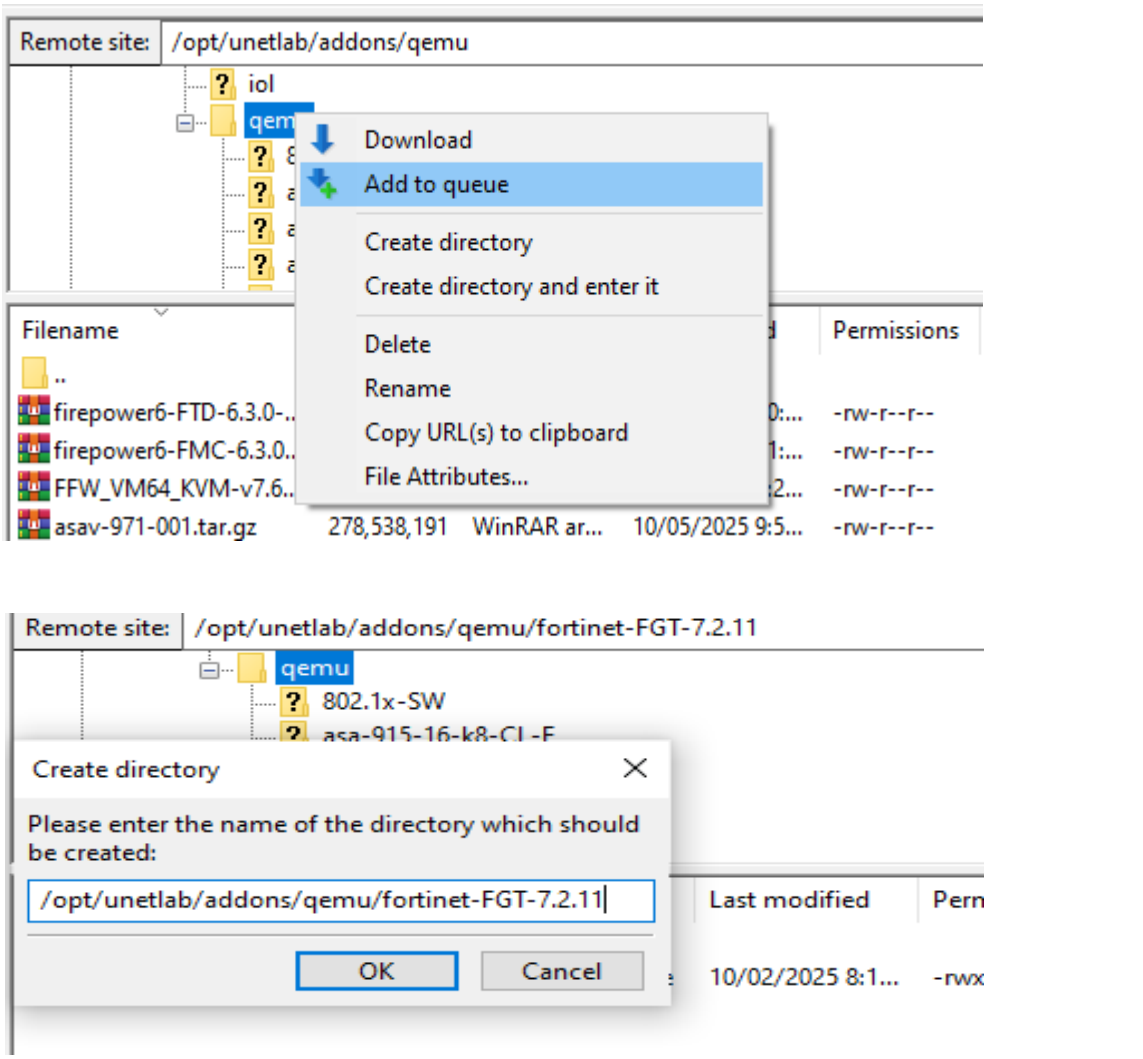


Figure 3.20: Integration du Firewall Fortigate-7.2.11 sur Eve-ng

(le fichier est nommé virtioa.qcow2)

Nous pouvons present verifier la disponibilite du firewall Fortigate sur Eve-ng. (Figure 3.21)

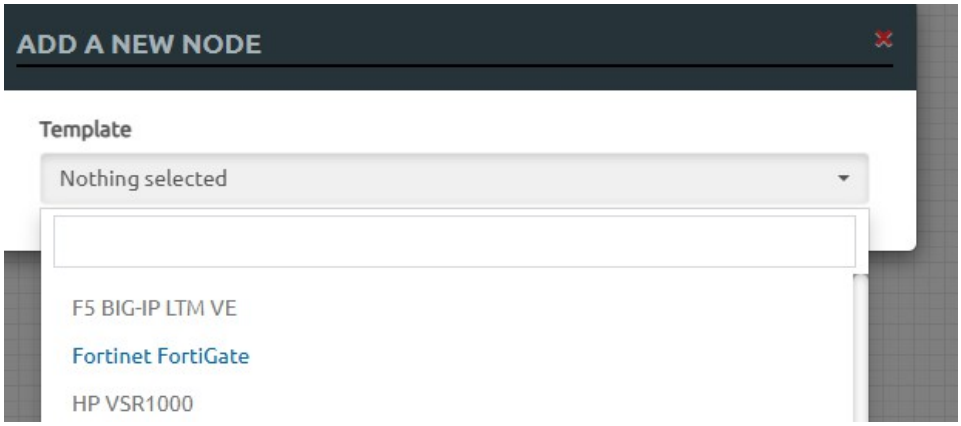


Figure 3.21: Visibilité du Firewall Fortigate sur Eve-ng

III.5.3 Obtention d'une licence d'évaluation Fortigate

Pour obtenir une licence d'évaluation FortiGate Firewall**,** il faudra aller sur : https://support.fortinet.com (inscription requise, créer un compte sur le portail FortiCloud), et télécharger le fichier de licence d'évaluation (FortiGate VM Eval License) qui active le Firewall pour 15 jours.

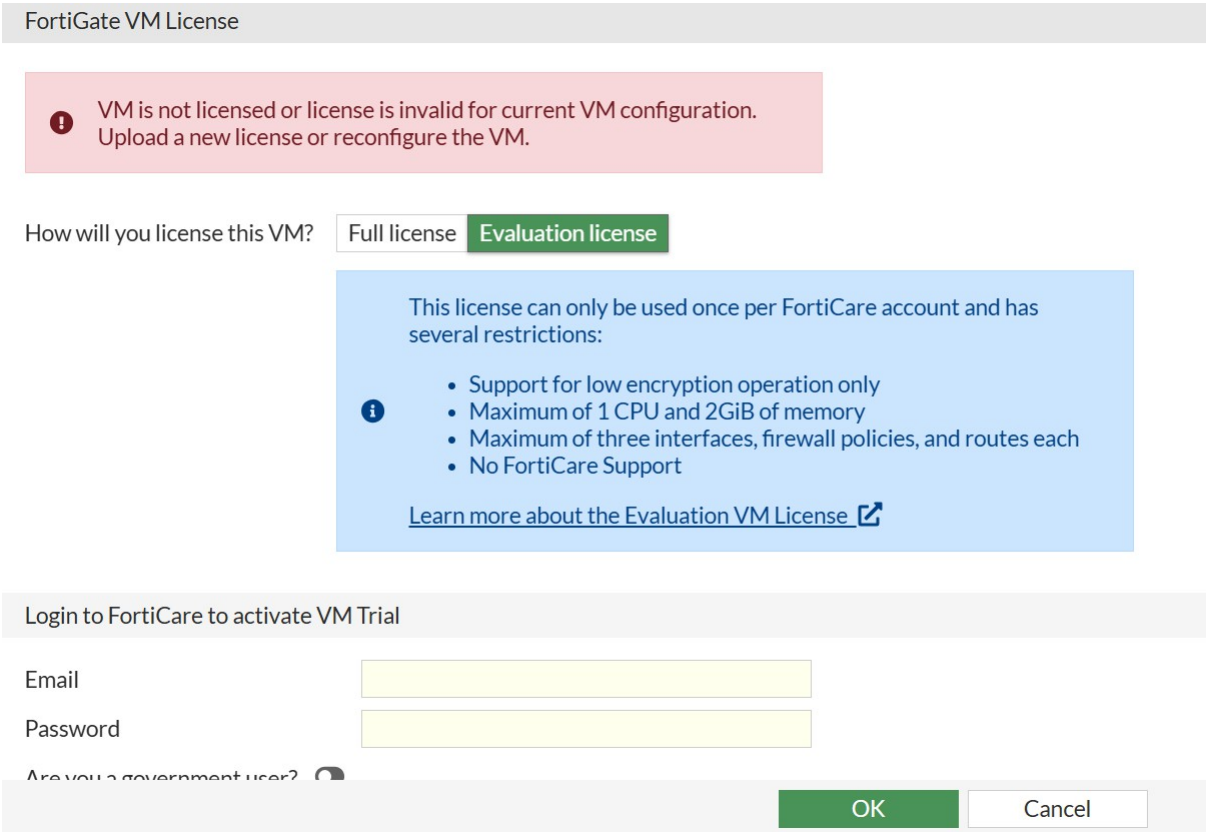


Figure 3.22: Téléchargement d'une licence d'évaluation Fortigate

III.6 Conclusion

Dans ce chapitre, nous avons pu voir en détails les différentes étapes techniques requises pour mettre en place notre plateforme de test. En effet, que ça soit l'installation de VMware Workstation, l'importation et la configuration de l'environnement EVE-NG ou l'utilisation de FileZilla pour le transfert SFTP des fichiers requis, ces démarches nous ont permis de préparer un environnement virtuel bien stable.

De plus, l'intégration du pare-feu FortiGate téléchargé depuis la plateforme officielle de Fortinet est une autre étape primordiale. En effet, il s'agit d'émuler un tel dispositif de sécurité dans le cadre d'un environnement maîtrisé. Sur ces bases, nous pourrons de toute évidence effectuer par la suite des configurations données de politiques de sécurité et tester les performances par simulation d'attaques.

Chapitre 4

Déploiement de Fortigate Firewall :

Configuration et scénarios de tests de validation

4

Déploiement de Fortigate Firewall : Configuration et scénarios de tests de validation

IV.1 Introduction

FortiGate est l'un des pare-feu réseau les plus largement déployés au monde. Il offre des fonctionnalités avancées de sécurité et de connectivité au sein d'une plateforme unifiée, centralisée via FortiGate Cloud.

Ce chapitre expose diverses configurations de politiques de sécurité, accompagnées de tests de validation, permettant de maîtriser l'art de la configuration, la gestion et le comportement des pare-feu FortiGate. Avant cela, nous allons présenter tout d'abord ses différents composants, les services de sécurité ainsi que les politiques de pare-feu associés.

IV.2 Composants du Firewall Fortigate

FortiGate est une plateforme de pare-feu nouvelle génération conçue pour offrir une sécurité et des performances réseau complètes. Son architecture est composée de plusieurs composants fonctionnant ensemble pour offrir une protection avancée contre les menaces, une segmentation du réseau et une connectivité sécurisée. Explorons chaque composant en détail :

IV.2.1 Unités de traitement (Processing Units)

IV.2.1.1 Unité centrale de traitement (CPU : Central Processing Unit)

Le processeur est l'unité centrale de traitement responsable de l'exécution des opérations de pare-feu, du traitement des paquets et de divers services de sécurité. FortiGate utilise des processeurs multicœurs pour gérer efficacement le trafic à haut débit et les fonctions de sécurité complexe.

IV.2.1.2 Processeur réseau (NP : Network Processor)

FortiGate intègre des processeurs réseau spécialisés, tels que les FortiASIC NP6 et NP7, dédiés au déchargement et à l'accélération de tâches spécifiques telles que le transfert de paquets, le

chiffrement/déchiffrement et le traitement de contenu. Ces puces NP améliorent les performances et l'évolutivité du pare-feu.

IV.2.2 Services de sécurité (Security Services)

a. Pare-feu (Firewall)

Le pare-feu applique les politiques de sécurité en inspectant et en filtrant le trafic réseau selon des règles prédéfinies, garantissant ainsi que seul le trafic autorisé circule sur le réseau.

b. IPS (Intrusion Prevention System)

Le module IPS détecte et prévient les attaques réseau connues et inconnues en analysant les schémas de trafic, les signatures et les anomalies de comportement, protégeant ainsi contre les exploits, les logiciels malveillants et les vulnérabilités.

c. VPN (Virtual Private Network)

FortiGate prend en charge diverses technologies VPN, notamment IPsec, SSL et L2TP, pour établir des canaux de communication sécurisés entre les sites distants, les utilisateurs et les partenaires sur des réseaux non fiables comme Internet.

d. Antivirus and Antimalware

FortiGate inclut des services antivirus et antimalware pour détecter et bloquer les logiciels malveillants, tels que les virus, les vers, les chevaux de Troie et les logiciels espions, les empêchant ainsi d'infecter le réseau.

e. Filtrage Web

La fonction de filtrage web contrôle l'accès aux sites web en fonction de catégories, d'URL ou de mots-clés, permettant aux organisations d'appliquer des politiques d'utilisation acceptables, de bloquer les sites malveillants et d'améliorer leur productivité.

f. Contrôle des applications

FortiGate offre des fonctionnalités de contrôle des applications pour identifier et contrôler l'utilisation de diverses applications au sein du réseau, permettant ainsi aux administrateurs de définir des politiques d'autorisation, de refus ou de limitation d'accès à des applications spécifiques.

g. Prévention de la perte de données

La fonctionnalité DLP empêche la transmission non autorisée de données sensibles hors du réseau en inspectant le trafic sortant à la recherche de modèles de données prédéfinis tels que les numéros de carte de crédit, les numéros de sécurité sociale ou la propriété intellectuelle.

h. Protection avancée contre les menaces FortiGate intègre des mécanismes avancés de protection contre les menaces, notamment le sandboxing et l'analyse comportementale, pour détecter et bloquer les menaces sophistiquées telles que les exploits zero-day et les attaques ciblées.

IV.2.3 Composants réseau

a. Interfaces

FortiGate comprend des interfaces réseau physiques et virtuelles pour se connecter à différents segments de réseau, permettant ainsi l'entrée/sortie du trafic et la segmentation du réseau pour une sécurité et une optimisation des performances.

b. Routage

FortiGate prend en charge les protocoles de routage dynamique et statique pour acheminer le trafic entre les différents segments de réseau de manière efficace et sécurisée, garantissant ainsi des performances et une connectivité réseau optimales.

c. VLANs (Virtual Local Area Networks)

Les VLAN permettent à FortiGate de segmenter le réseau en plusieurs LAN virtuels, isolant ainsi le trafic et améliorant la sécurité, l'évolutivité et les performances sur des réseaux vastes et complexes.

IV.2.4 Gestion et rapports

a. Interface de gestion

Le firewall Fortigate fournit deux modes d’accès : CLI et GUI. L'interface de ligne de commande (CLI) du pare-feu FortiGate offre aux administrateurs un outil puissant et flexible pour configurer, surveiller et dépanner le pare-feu.

Elle est accessible via SSH ou via le port console directement connecté au pare-feu. Elle fournit une interface textuelle permettant aux administrateurs d'exécuter des commandes pour effectuer diverses tâches liées à la configuration et à la gestion du pare-feu. (Figure 4.1)

```
System is starting...
Formatting shared data partition ... done!
Starting system maintenance...
Scanning /dev/vda1... (100%)
Scanning /dev/vda2... (100%)
Serial number is FFVMEVYIF-Y2-J07


FortiFirewall-VM64-KVM login: admin
Password:
Verifying password...

You are forced to change your password. Please input a new password.
New Password:
Confirm Password:

FortiFirewall-VM64-KVM login:

FortiFirewall-VM64-KVM login: admin
Password:
Verifying password...

You are forced to change your password. Please input a new password.
New Password:
Confirm Password:
Verifying password...
Welcome!

FortiFirewall-VM64-KVM #
```

```
FortiFirewall-VM64-KVM # show system interface
config system interface
    edit "port1"
        set vdom "root"
        set mode dhcp
        set allowaccess ping https ssh http
        set type physical
        set snmp-index 1
    next
    edit "port2"
        set vdom "root"
        set type physical
        set snmp-index 2
    next
    edit "port3"
        set vdom "root"
        set type physical
        set snmp-index 3
    next
    edit "port4"
        set vdom "root"
        set type physical
        set snmp-index 4
    next
    edit "naf.root"
--More--
```

Figure 4.1: Interface CLI du Firewall Fortigate

D’autre part, l'accès à l'interface utilisateur graphique (GUI) d'un pare-feu FortiGate permet aux administrateurs de configurer et de gérer le pare-feu via une interface web. Connaissant l’adresse Ip du port de gestion (management port), nous pouvons y accéder via un navigateur.

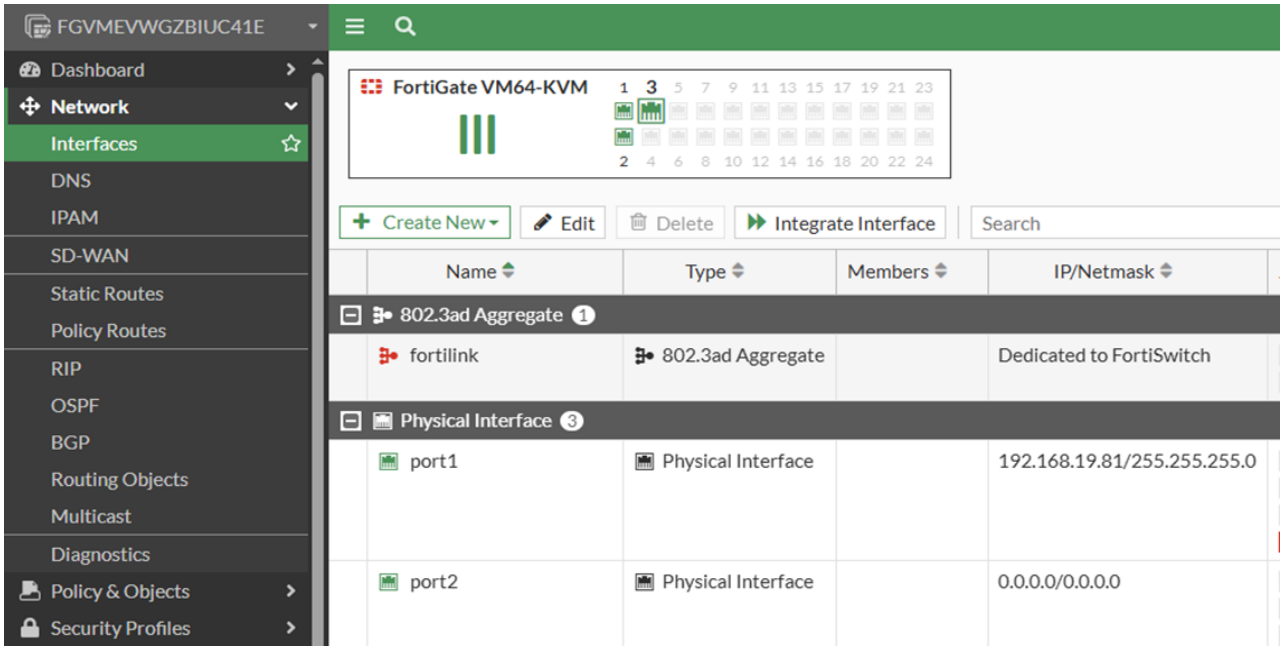


Figure 4.2: Interface GUI du Firewall Fortigate

b. Journalisation et rapports

FortiGate enregistre l'activité réseau, les événements de sécurité et les violations de politiques, générant des rapports et des alertes détaillés permettant aux administrateurs d'analyser les incidents de sécurité, de résoudre les problèmes et de maintenir la conformité aux exigences réglementaires.

IV.2.5 Présentation des politiques de pare-feu

Les politiques de pare-feu sont des règles qui régissent le flux de trafic à travers le pare-feu. Chaque politique comprend des conditions, des actions et des profils de sécurité. Les politiques sont évaluées séquentiellement, et la première politique correspondante est appliquée au trafic.

IV.2.5.1 Conditions de la politique

- Source et Destination : Spécifiez les adresses IP ou les groupes d'adresses source et de destination du trafic.
- Service : Définissez le protocole et le numéro de port ou le groupe de services utilisés par le trafic.
- Planification (Schedule) : Vous pouvez également restreindre l'activation de la stratégie selon une planification définie.
- Action : Indiquez si le trafic est autorisé, refusé ou journalisé.

IV.2.5.2 Actions de la politique

- Accepter (Accept) : Autoriser le trafic à traverser le pare-feu.
- Refuser (Deny) : Bloquer le trafic et générer une entrée de journal.
- Surveiller (Monitor) : Journaliser le trafic, mais l'autoriser à traverser le pare-feu.

IV.2.5.3 Profils de sécurité

- Antivirus : Analysez vos fichiers à la recherche de virus et de logiciels malveillants.
- Système de prévention des intrusions (IPS) : Détectez et prévenez les attaques réseau.
- Filtrage Web : Bloquez l'accès aux sites web malveillants ou inappropriés.
- Contrôle des applications : Contrôlez l'accès à des applications et protocoles spécifiques.

IV.2.5.4 Règle par défaut et Politique implicite de refus total

Le pare-feu FortiGate suit la règle par défaut : le trafic non conforme à une politique de pare-feu est implicitement refusé. Ce comportement garantit que seul le trafic explicitement autorisé peut traverser le pare-feu, renforçant ainsi la sécurité du réseau.

Par défaut, le pare-feu FortiGate inclut une politique implicite « Refuser tout » à la fin de la liste des politiques. Cette politique refuse tout trafic qui ne correspond pas à une politique précédente. Les administrateurs peuvent modifier ce comportement en ajoutant des politiques d'autorisation spécifiques au-dessus de la politique « Refuser tout ».

IV.3 Création d'une politique de sécurité dans FortiGate Firewall

Scénario : Nous allons autoriser le trafic du réseau local vers Internet. Nous allons définir une politique de sécurité autorisant le trafic du port 2 vers le port 1 (Figure 4.3). VPC (réseau local) pourra alors accéder à Internet.

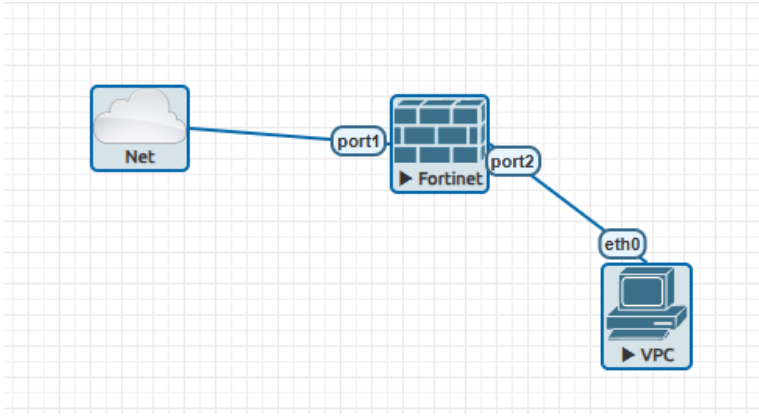


Figure 4.3: Topologie de test - Connexion Internet

```
FortiGate-VM64-KVM # sh sys interface
name    Name.
fortilink   static   0.0.0.0 0.0.0.0  10.255.1.1 255.255.255.0  up   disable   aggregate
l2t.root   static   0.0.0.0 0.0.0.0  0.0.0.0 0.0.0.0  up   disable   tunnel
naf.root   static   0.0.0.0 0.0.0.0  0.0.0.0 0.0.0.0  up   disable   tunnel
port1   dhcp   0.0.0.0 0.0.0.0  192.168.43.83 255.255.255.0  up   disable   physical
port2   static   0.0.0.0 0.0.0.0  0.0.0.0 0.0.0.0  up   disable   physical
port3   static   0.0.0.0 0.0.0.0  0.0.0.0 0.0.0.0  up   disable   physical
port4   static   0.0.0.0 0.0.0.0  0.0.0.0 0.0.0.0  up   disable   physical
ssl.root   static   0.0.0.0 0.0.0.0  0.0.0.0 0.0.0.0  up   disable   tunnel

FortiGate-VM64-KVM # sh sys interface
```

Figure 4.4 : Affichage des paramètres réseau du Fortigate Firewall

On note l'adresse IP (192.168.43.83) du port 1 de gestion (management) du Pare-feu.

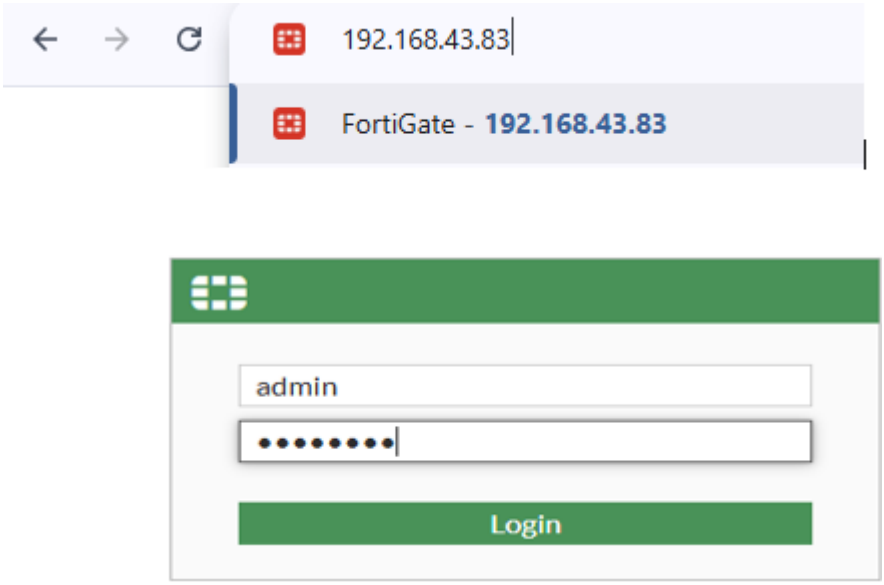
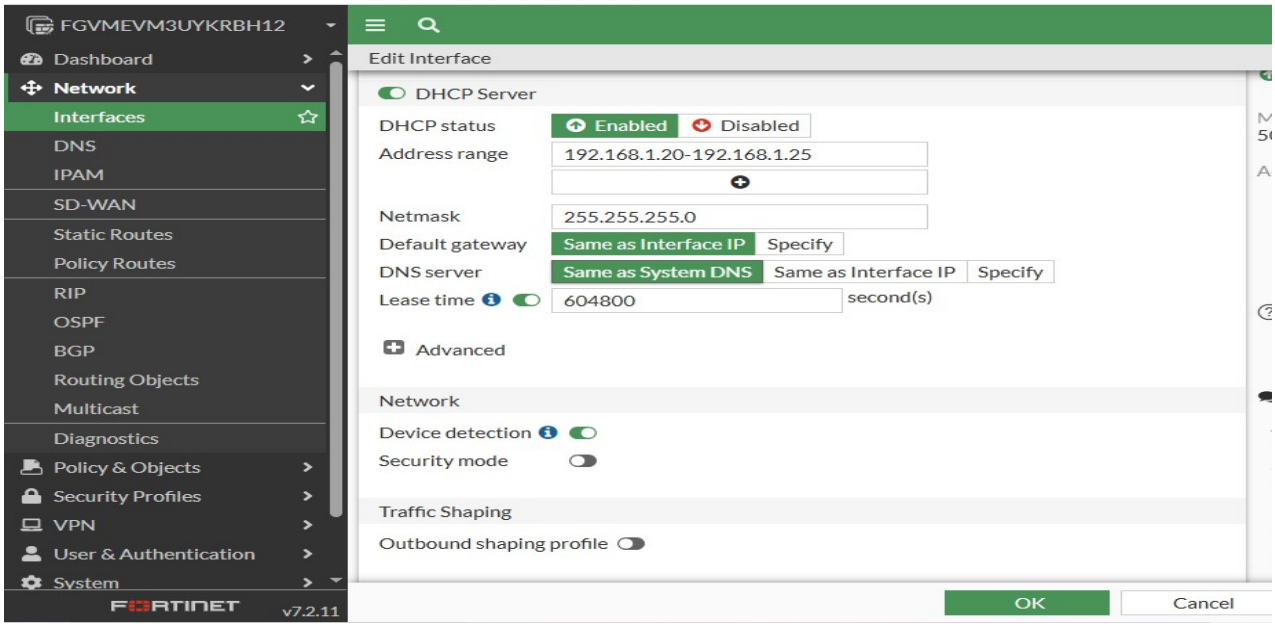


Figure 4.5 : Accès à l'interface graphique du Pare-feu

1. Nous allons sur **Network > Interfaces** > Port2, nous définissons l'adresse IP de l'interface (192.168.1.1/24) et nous configurons le serveur DHCP sur l'interface Port2 (la plage d'adresses IP est : 192.168.1.20 à 192.168.1.25.



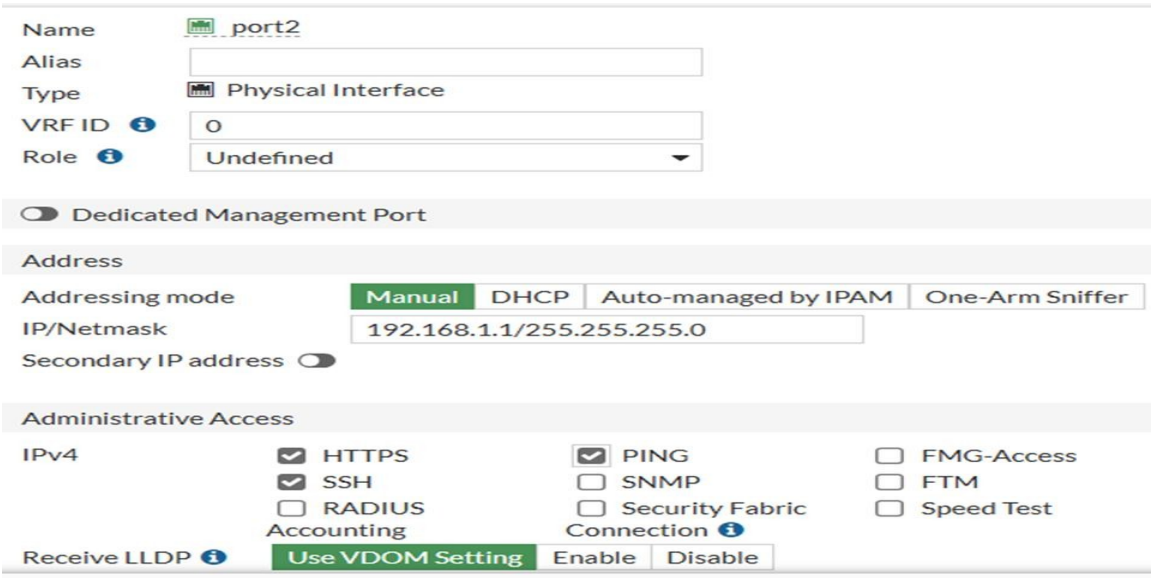


Figure 4.6 : Configuration du Port 2

2. Nous allons sur la section **Policy & Objects > Firewall Policy** section, on clique sur **Create New** pour ajouter une nouvelle stratégie de pare-feu, puis on configure les paramètres suivants :

Name	**Internet**
Incoming Interface	**Port 2**
Outgoing Interface	**Port 1**
Source	**mon local**
Destination	**all**
Schedule	**Always**
Service	**All**
Action	**Accept**

Tableau 4.1 : Paramètres de configuration de la politique du pare-feu

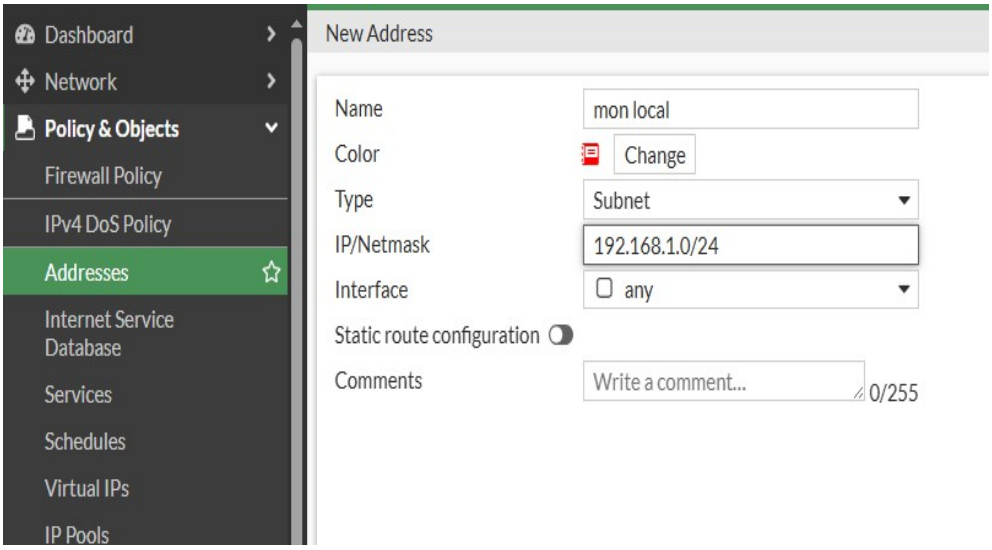


Figure 4.7 : Définition du sous réseau local (mon local)

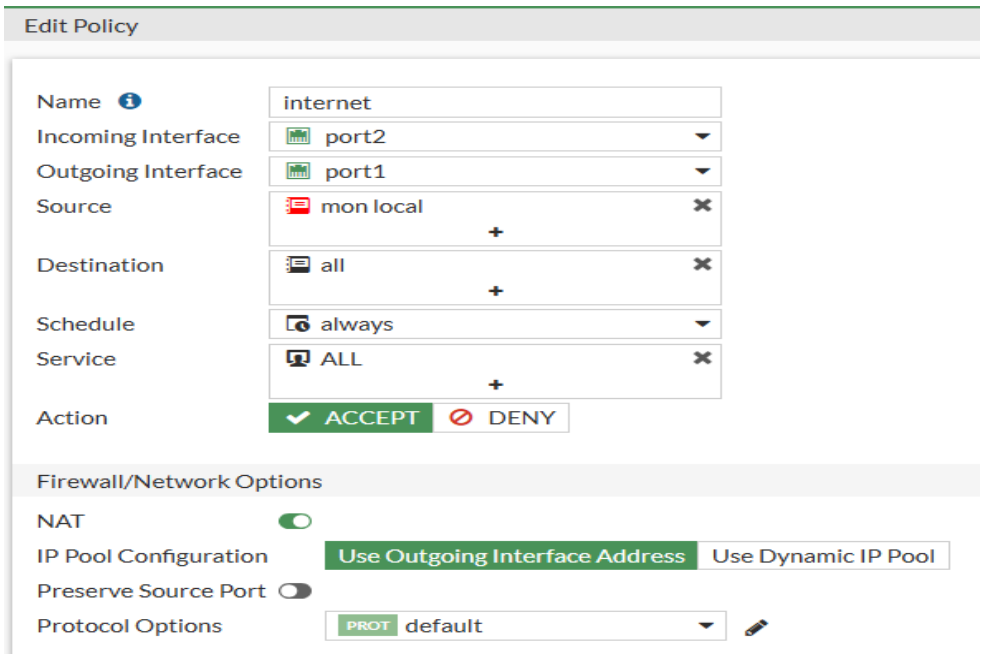


Figure 4.8 : Définition de la politique Internet

Nous pouvons voir apparaitre sur la figure 4.9 notre politique « Internet » en première ligne, ensuite vient la politique implicite « Refuser tout ».

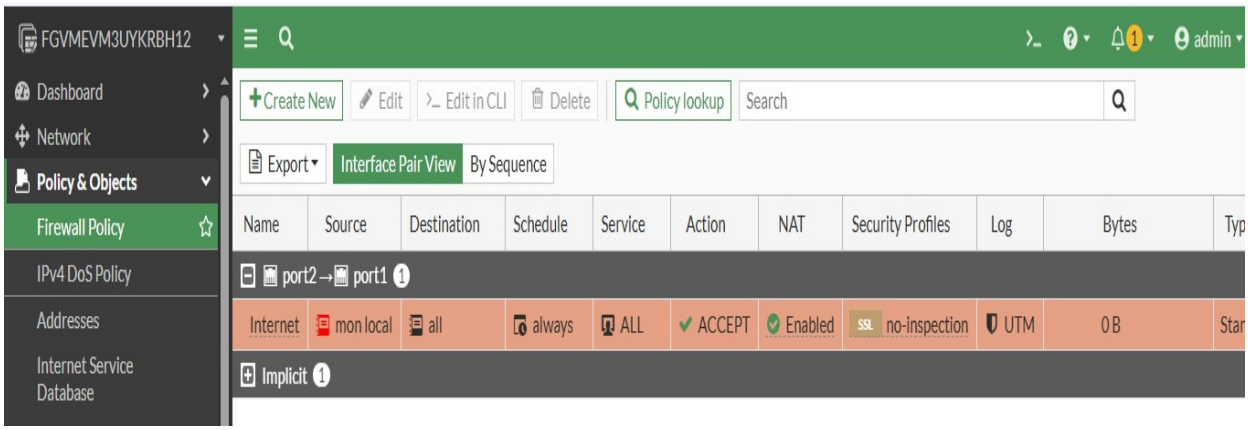


Figure 4.9 : Affichage de la politique définie (Internet)

3. Ensuite, sur VPC on configure celui-ci comme client DHCP afin d'obtenir une adresse IP automatiquement. Une fois cela fait, nous procédons à un test pour vérifier l'accès à Internet (Figure 4.10).

```
VPCS> sh ip

NAME        : VPCS[1]
IP/MASK     : 0.0.0.0/0
GATEWAY     : 0.0.0.0
DNS         :
MAC         : 00:50:79:66:68:04
LPORT       : 20000
RHOST:PORT  : 127.0.0.1:30000
MTU         : 1500

VPCS> dhcp
DDD
Can't find dhcp server

VPCS> dhcp
DDORA IP 192.168.1.20/24 GW 192.168.1.1

VPCS>
```

Figure 4.10 : Configuration VPC

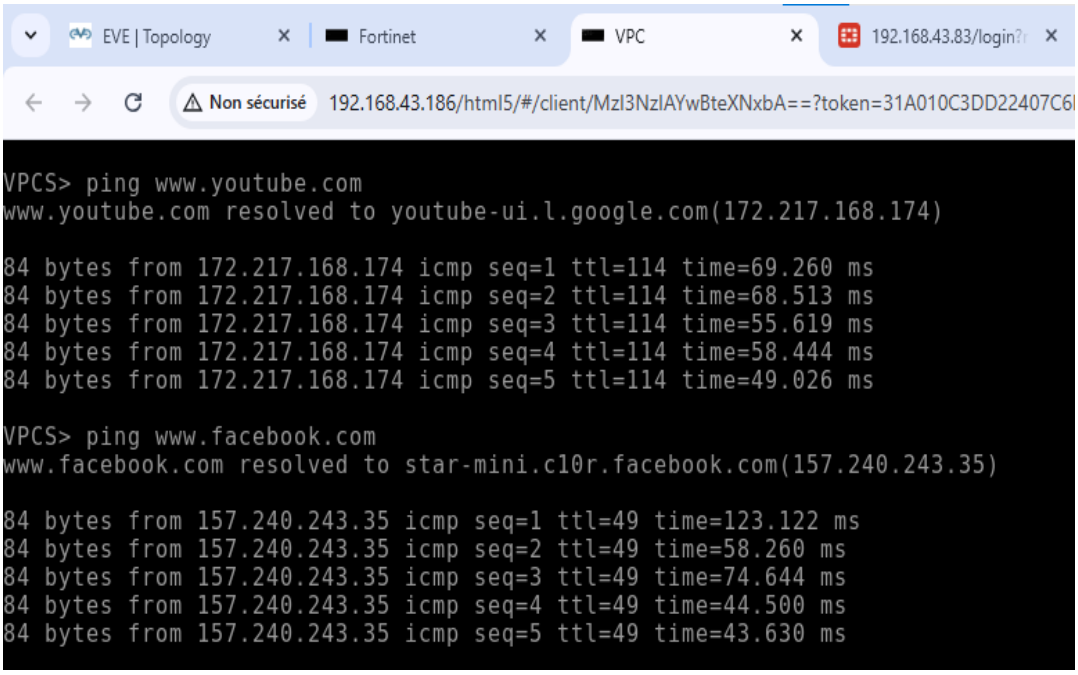


Figure 4.11 : Résultat du test d'accès à Internet

4. Nous allons maintenant bloquer l'accès à Internet en suivant la configuration suivante :

Name	**Blockage**
Incoming Interface	**Port 2**
Outgoing Interface	**Port 1**
Source	**mon local**
Destination	**all**
Schedule	**Always**
Service	**Ping**
Action	**Deny**

Tableau 4.2 : Paramètres de configuration de la politique Blockage

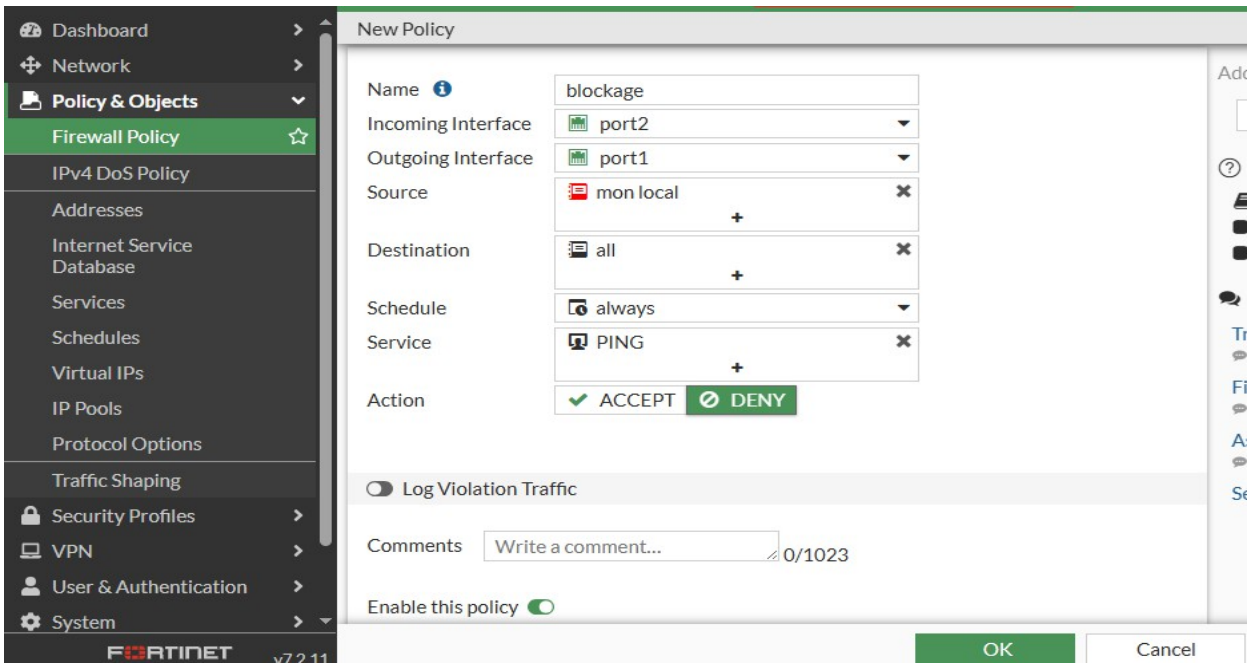


Figure 4.12 : Configuration de la politique de blocage

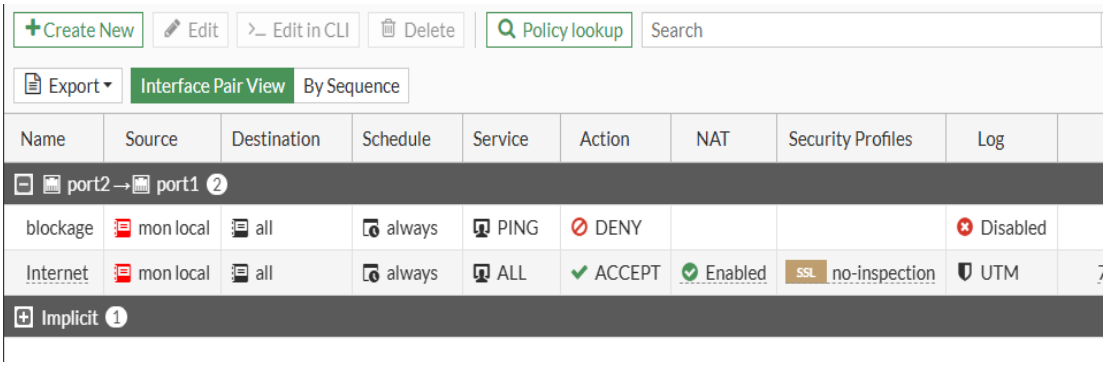


Figure 4.13 : Priorité de la politique de blocage

La figure 4.14 montre le résultat du test réussi.

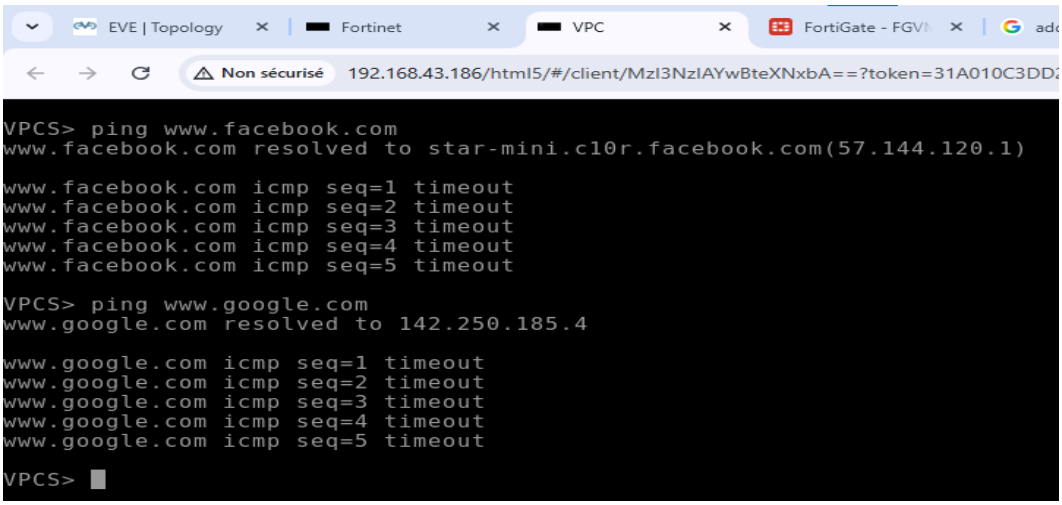


Figure 4.14 : Résultat du test de la politique de blocage

IV.4 Création d'un profile de sécurité de Contrôle d'applications

1. Sur **Security Profile section > Application Control**.

- On crée un nouveau **Application Control**
- Name: **block-réseaux sociaux**
- Dans les catégories, on bloque **Social Media, Video/Audio**

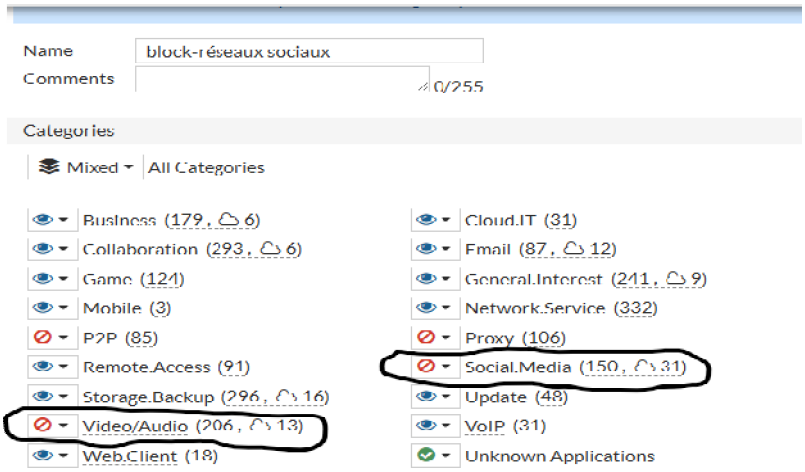


Figure 4.15 : Blocage des réseaux sociaux et video/audio

2. Sur **Application and Filter overrides > Create a new**.

- On selectionne **Application**
- Action**: Block**
- Application: **YouTube**

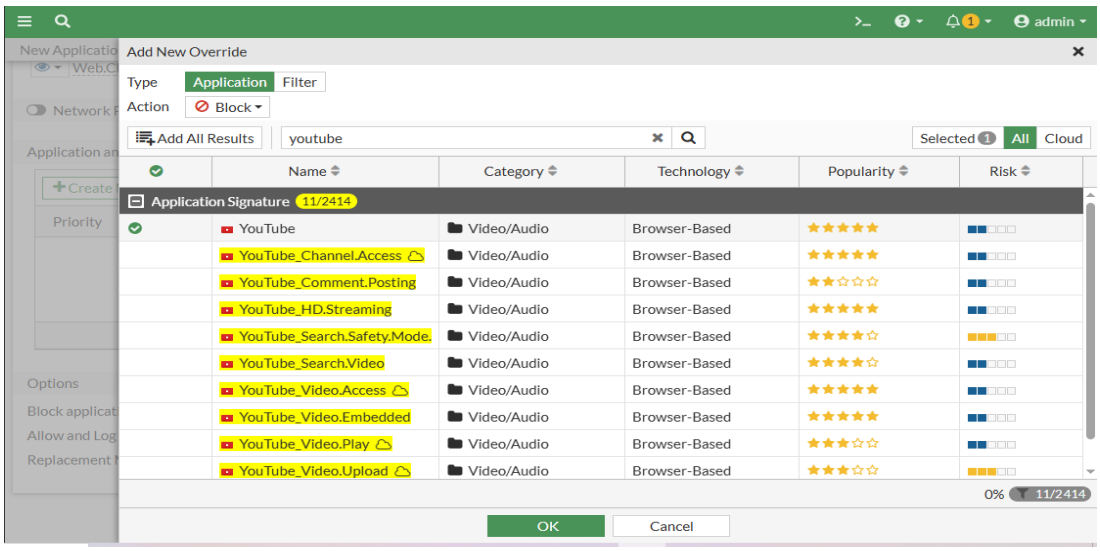


Figure 4.16 : Blocage de YouTube

3. Toujours sur **Application and Filter overrides > Create a new**.

- On selectionne **Application**
- Action: **Block**
- Application: **facebook**

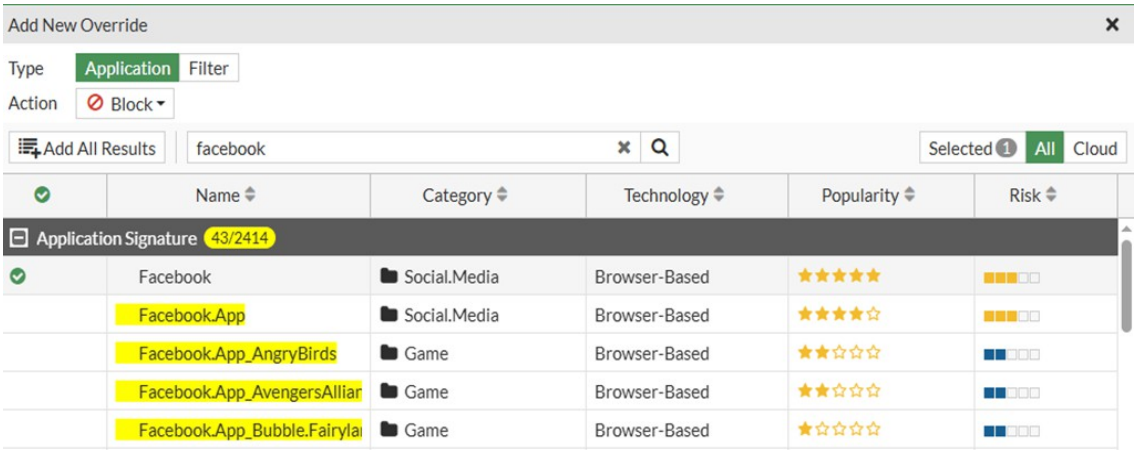


Figure 4.17 : Blocage du Facebook

La figure 4.18 montre le résultat de test réussi du blocage des réseaux sociaux apartir d'un poste Windows.

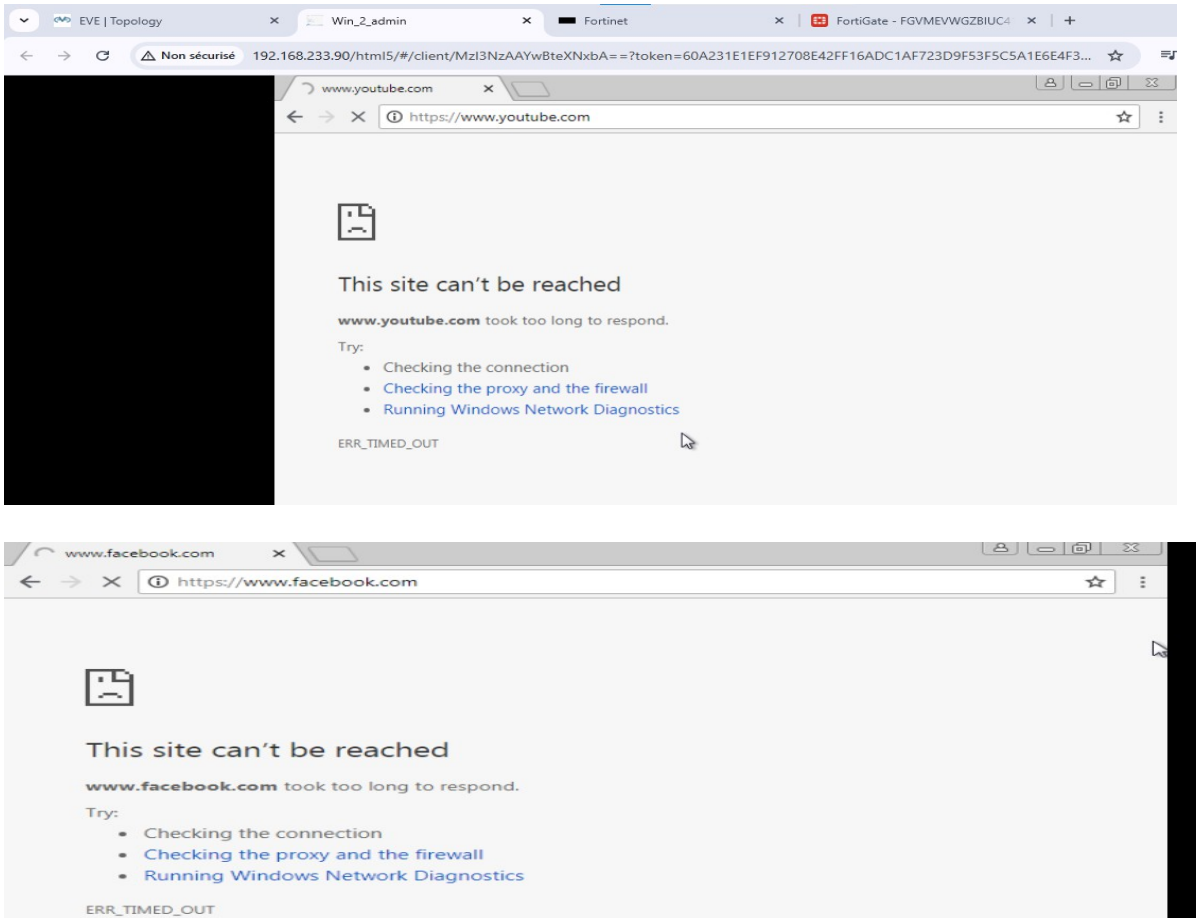


Figure 4.18 : Résultat du test de blocage des réseaux sociaux

IV.5 Création d'un portail d'authentification

Scénario : Nous prévoyons d'activer le portail d'authentification sur le port 2. Ensuite, lorsque les utilisateurs souhaitent se connecter à Internet, ils doivent d'abord saisir leur nom d'utilisateur et leur mot de passe, puis ils sont autorisés à naviguer sur Internet.

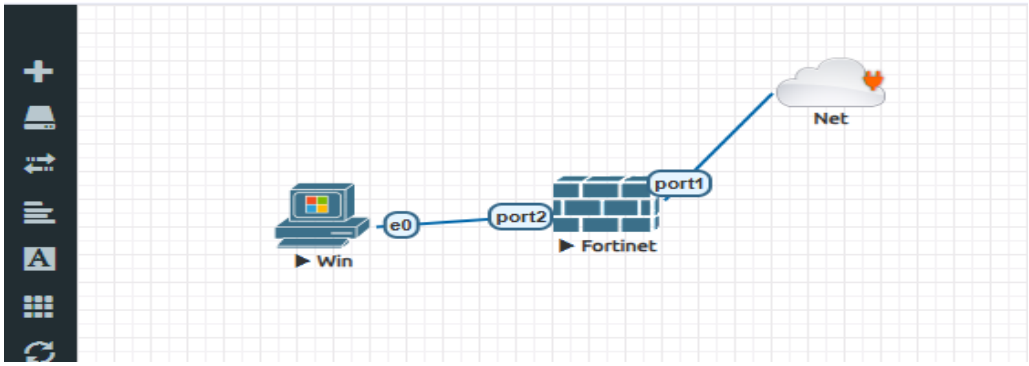


Figure 4.19 : Topologie pour le test du portail d'authentification

1. On définit une route statique **Static Routes** dans le pare-feu. Il est toujours recommandé de définir la route par défaut dans le pare-feu (0.0.0.0 0.0.0.0 Adresse IP Internet).

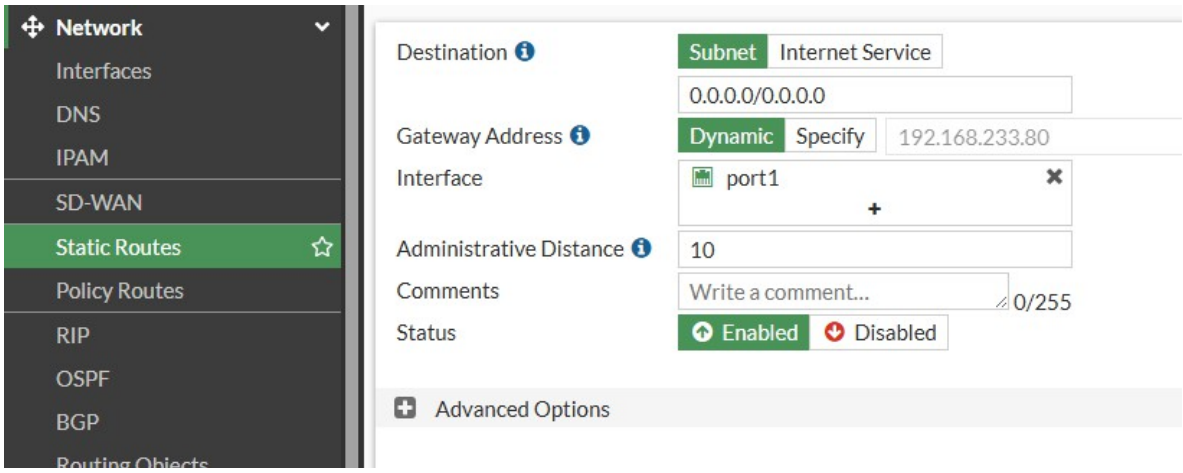


Figure 4.20 : Configuration de la route statique

2. On définit une politique de pare-feu du **port2 vers port1**, comme suit :

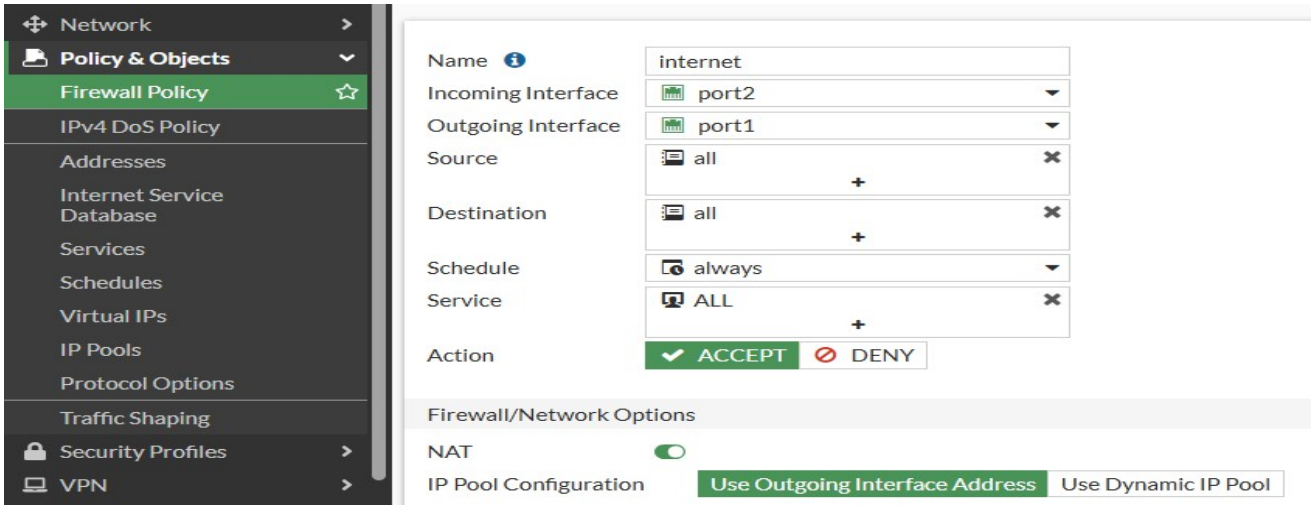


Figure 4.21 : Politique de pare-feu du **port2 vers port1**

3. On crée un utilisateur et un groupe. Sur **User & Authentication > User Groups** On crée un groupe nommé : **c.portal.**

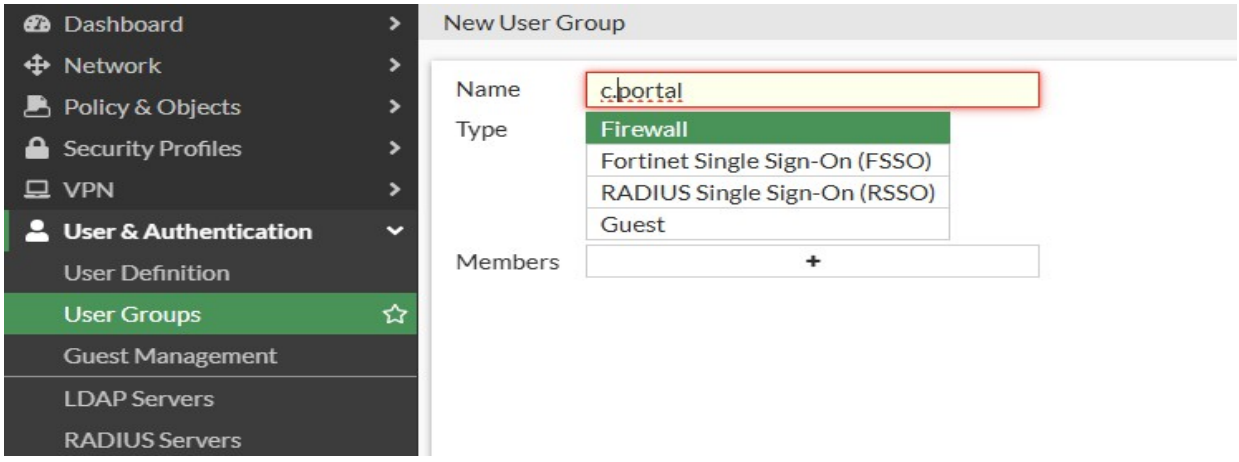


Figure 4.22 : Création du groupe d'utilisateurs c.portal

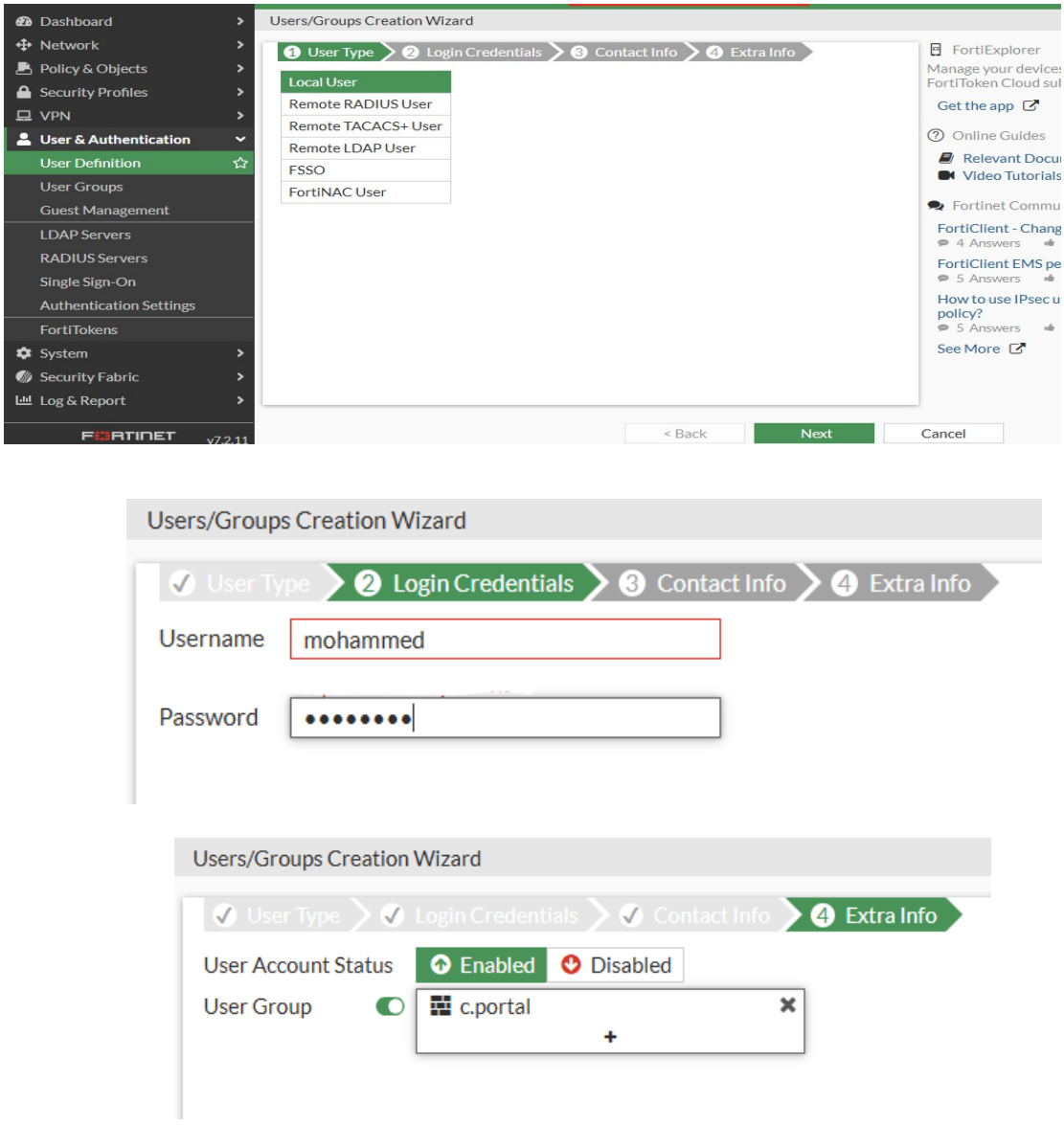


Figure 4.23 : Création d'un utilisateur

4. Sur **Network > Interfaces and edit port 2**. Dans la section Contrôle d'admission, on définit :
   - Mode de sécurité : **Captive Portal.**
   - Portail d'authentification : **Local.**
   - Accès utilisateur : Restreint au groupe et on assigne le groupe qu'en a créé à l'étape précédente.

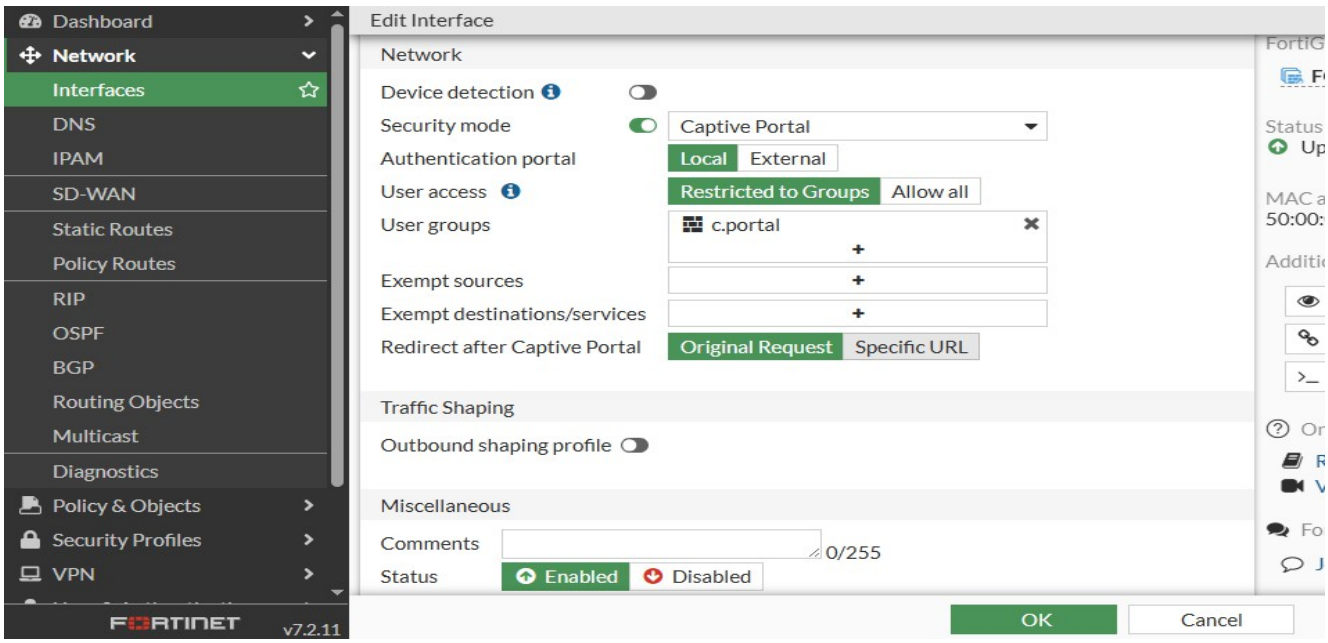


Figure 4.24 : Configure du portail d'authentification sur le port 2

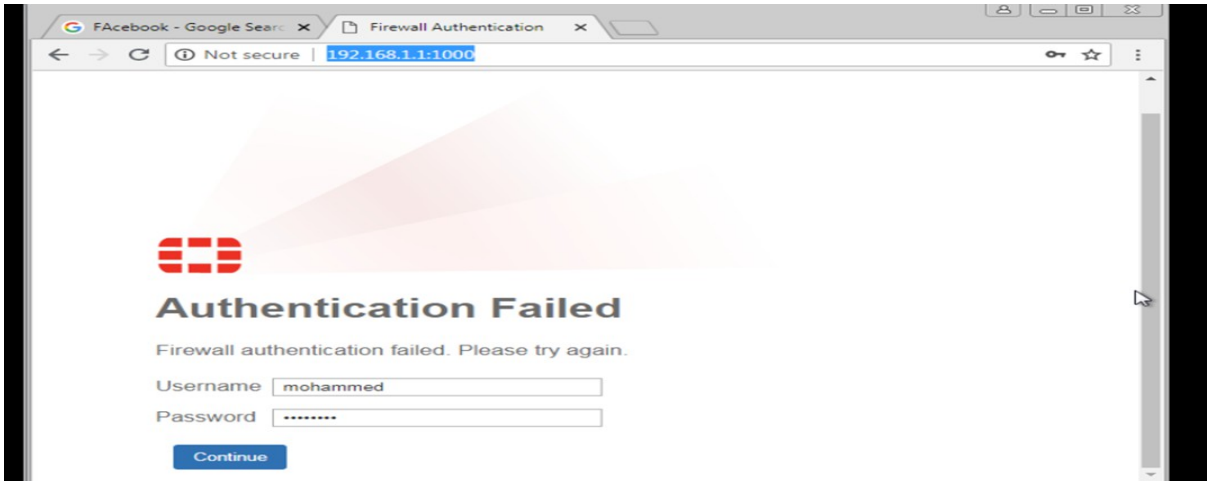


Figure 4.25 : Vérification du portail d'authentification

IV.6 Configuration d'un profil de prévention DDoS

Scénario : Nous allons configurer une prévention DDoS sur le trafic du port 3 vers le port 2. Nous allons lancer l'attaque DOS depuis VPC, et dans le pare-feu, on va définir une stratégie de prévention DDoS pour bloquer le trafic DOS.

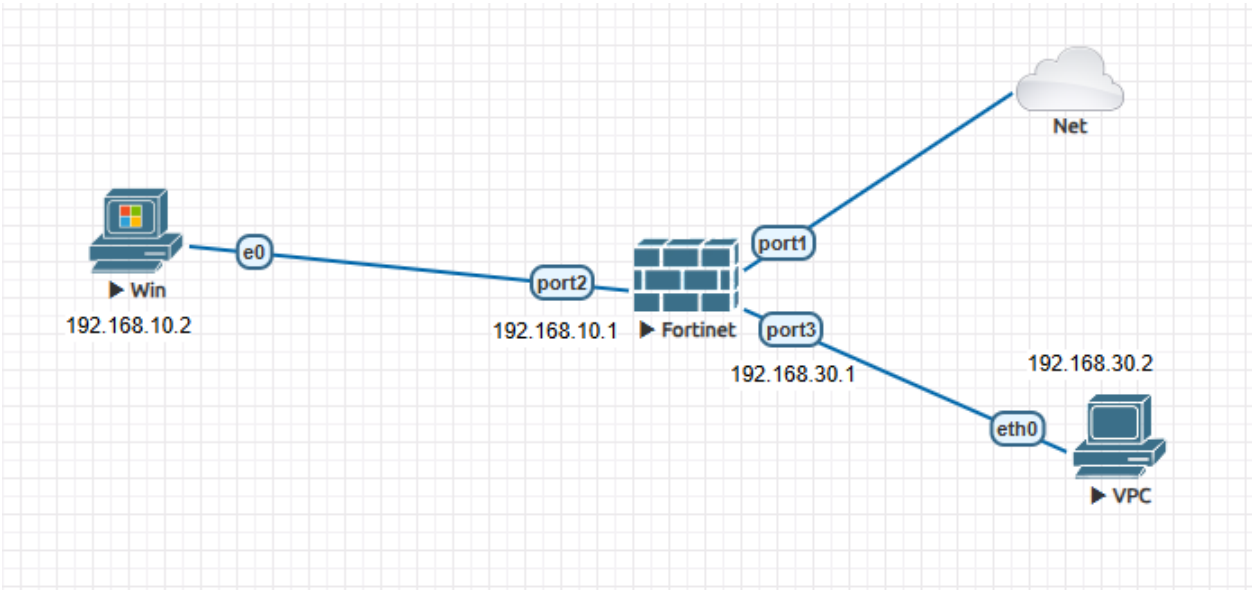


Figure 4.26 : Topologie de test du Profil de prévention DDoS

1. Tout d'abord, nous créons une stratégie pare-feux **(firewall policy)** du port 3 vers le port 2.

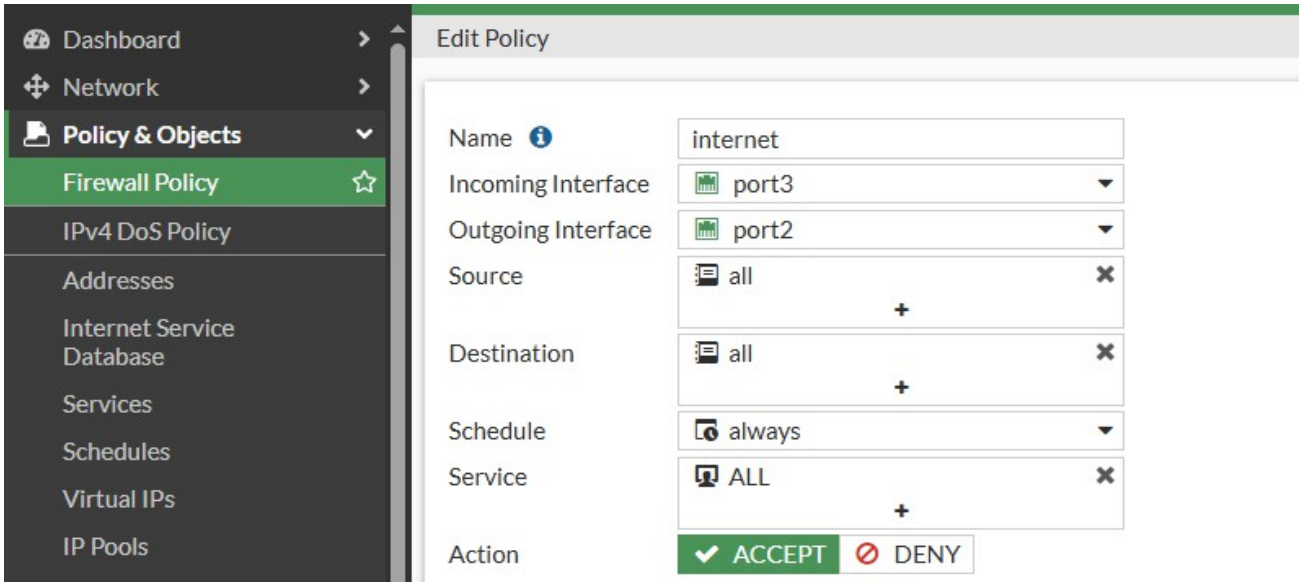
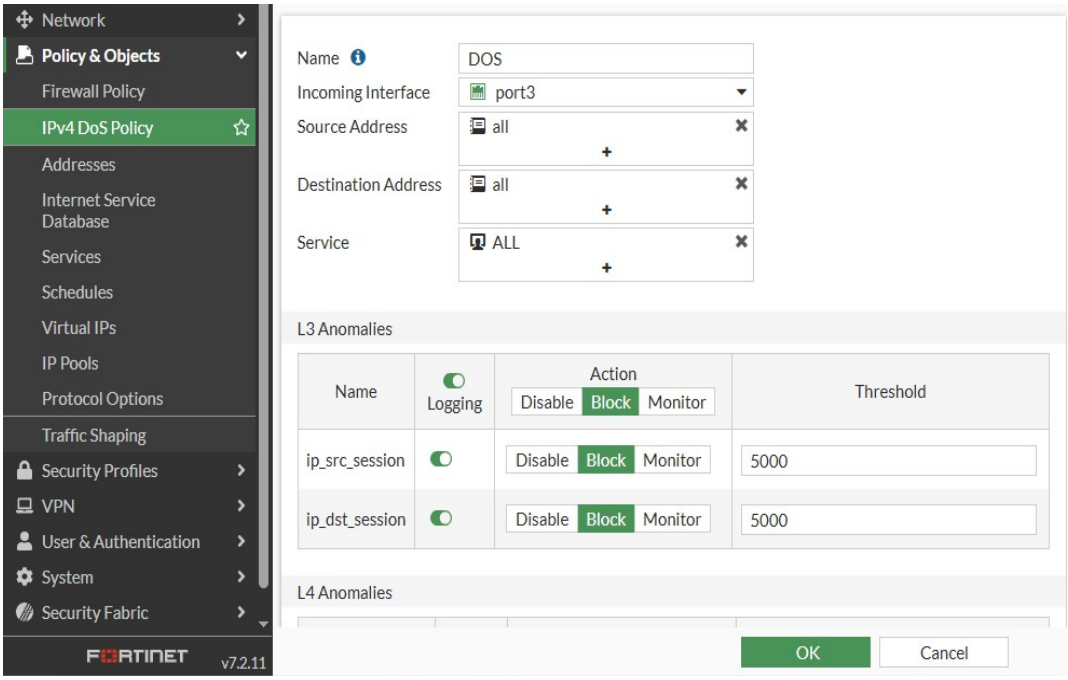


Figure 4.27 : Politique de pare-feu du port 3 vers le port 2

2. Sur **Policy & Object > IPV4 DOS Policy**, on introduit les paramètres suivants :

Name	**DOS**
Incoming interface	**Port 3**
Source, destination, Service	**All**
L3 Anomalies	**Logging: Enable** **Action : Block**
L4 Anomalies	**Logging : Enable** **Action : Block**

Tableau 4.3 : Paramètres de configuration de la politique DOS



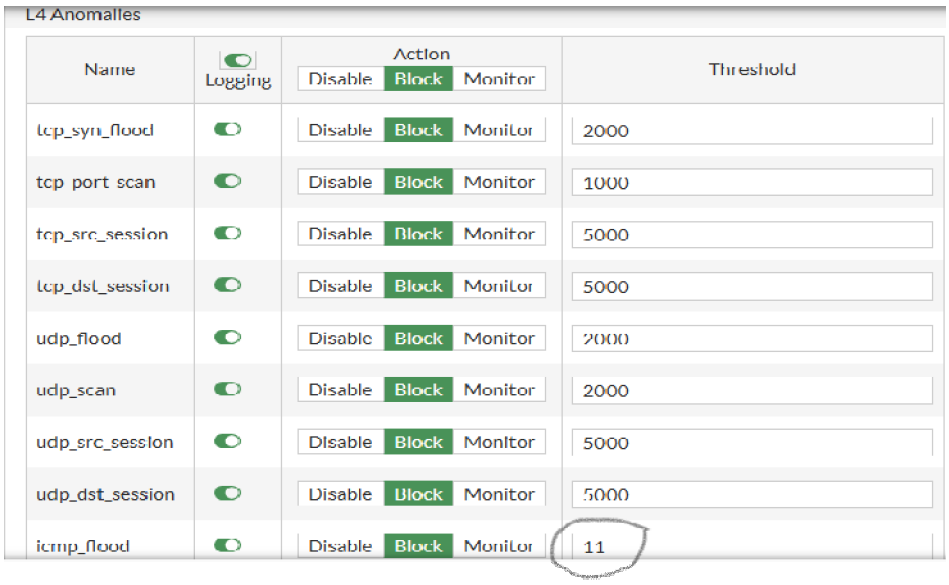


Figure 4.28 : IPV4 DOS Policy

Nous avons spécifié pour le threshold d'icmp_flood la valeur 11, ce qui permet de contrer toute attaque de type icmp flooding.

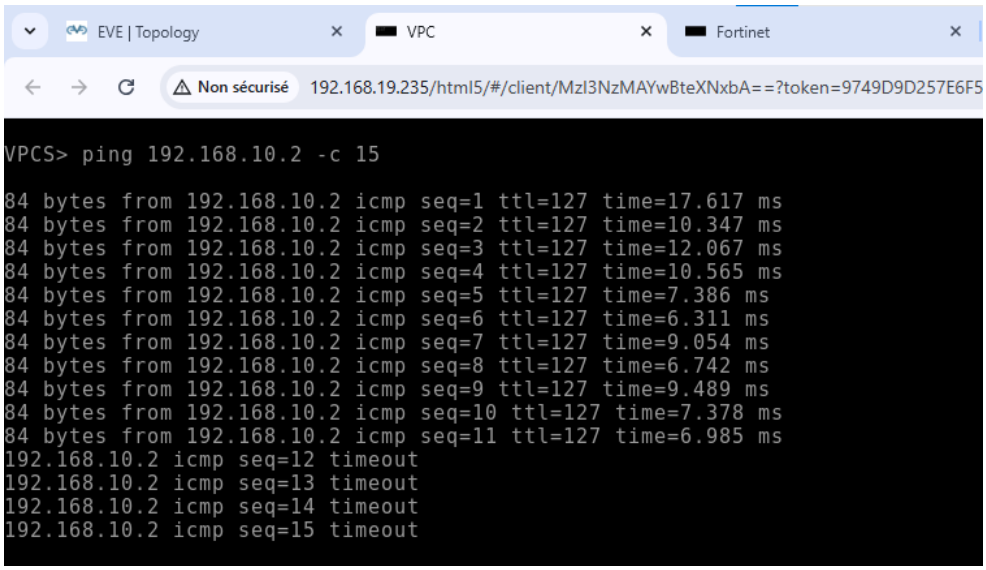


Figure 4.29 : Résultat de DDOS Prevention

IV.7 Configuration des profils d'antivirus, de prévention d'intrusion et de filtrage de fichiers

a) Antivirus

Objectif : L'antivirus analyse le trafic réseau à la recherche de logiciels malveillants, de virus et autres contenus malveillants connus, protégeant ainsi les terminaux et les réseaux contre les infections.

Fonctionnalités : Analyse antivirus en temps réel, analyse heuristique, détection basée sur les signatures, mise en quarantaine et suppression des fichiers infectés, et mises à jour automatiques des définitions antivirus.

Pour le filtrage antivirus, une licence valide est requise.

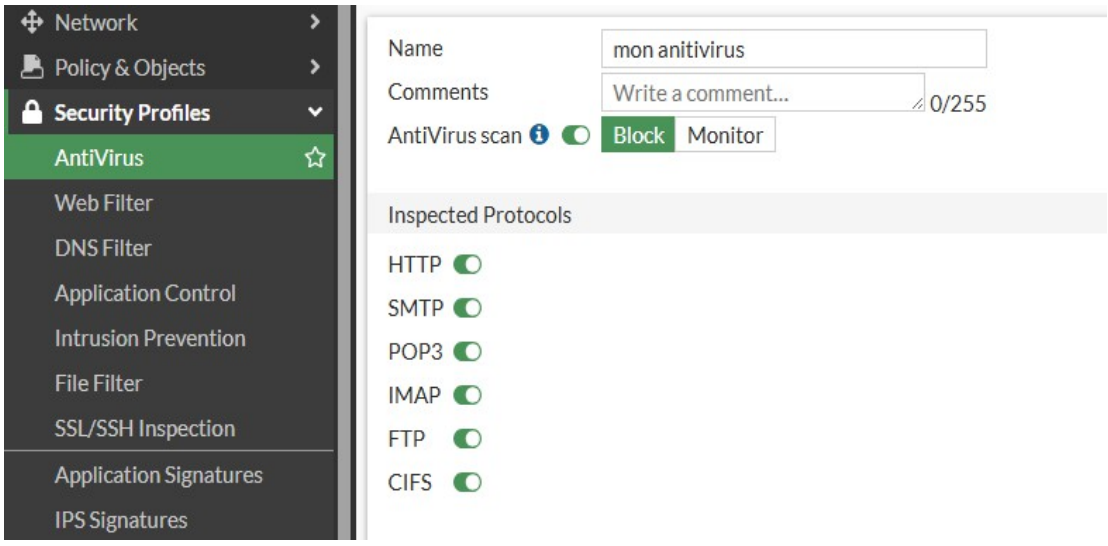


Figure 4.30 : Activation de l'Antivirusdd

b) File Filter

Objectif : Le filtre de fichiers analyse les transferts de fichiers à la recherche de logiciels malveillants, de contenu malveillant et de types de fichiers non autorisés, contribuant ainsi à prévenir la propagation des logiciels malveillants et à appliquer les politiques de prévention des pertes de données.

Fonctionnalités : Filtrage des types de fichiers, analyse antivirus des transferts de fichiers, mise en quarantaine et blocage des fichiers infectés et contrôle granulaire des types de fichiers autorisés.

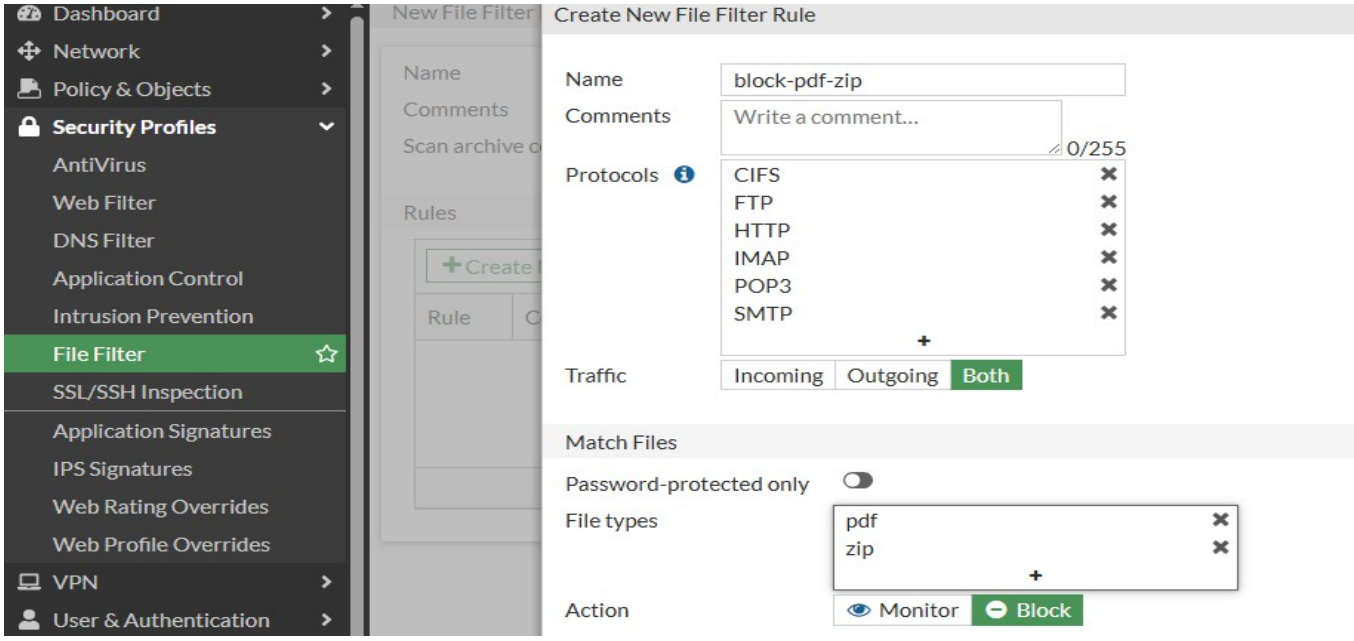


Figure 4.31 : Application du profil de sécurité « File Filter »

c) Prévention des intrusions

Objectif : Le système de prévention des intrusions (IPS) identifie et bloque les attaques réseau, notamment les exploits, les vulnérabilités et les schémas de trafic malveillants, afin de prévenir les accès non autorisés et les violations de données.

Fonctionnalités : Détection basée sur les signatures, détection basée sur les anomalies, inspection des protocoles, détection des anomalies de trafic et blocage des vecteurs d'attaque connus.

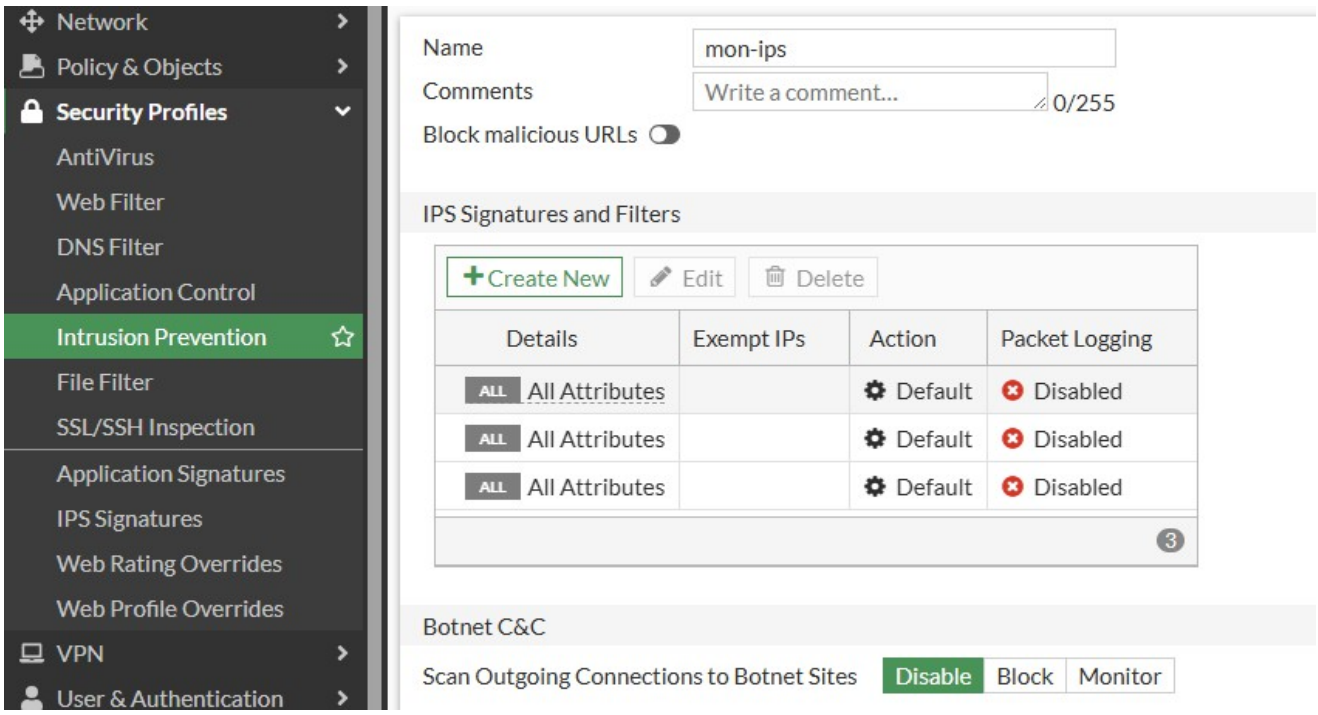


Figure 4.32 : Application du profil de sécurité « Intrusion Prevention »

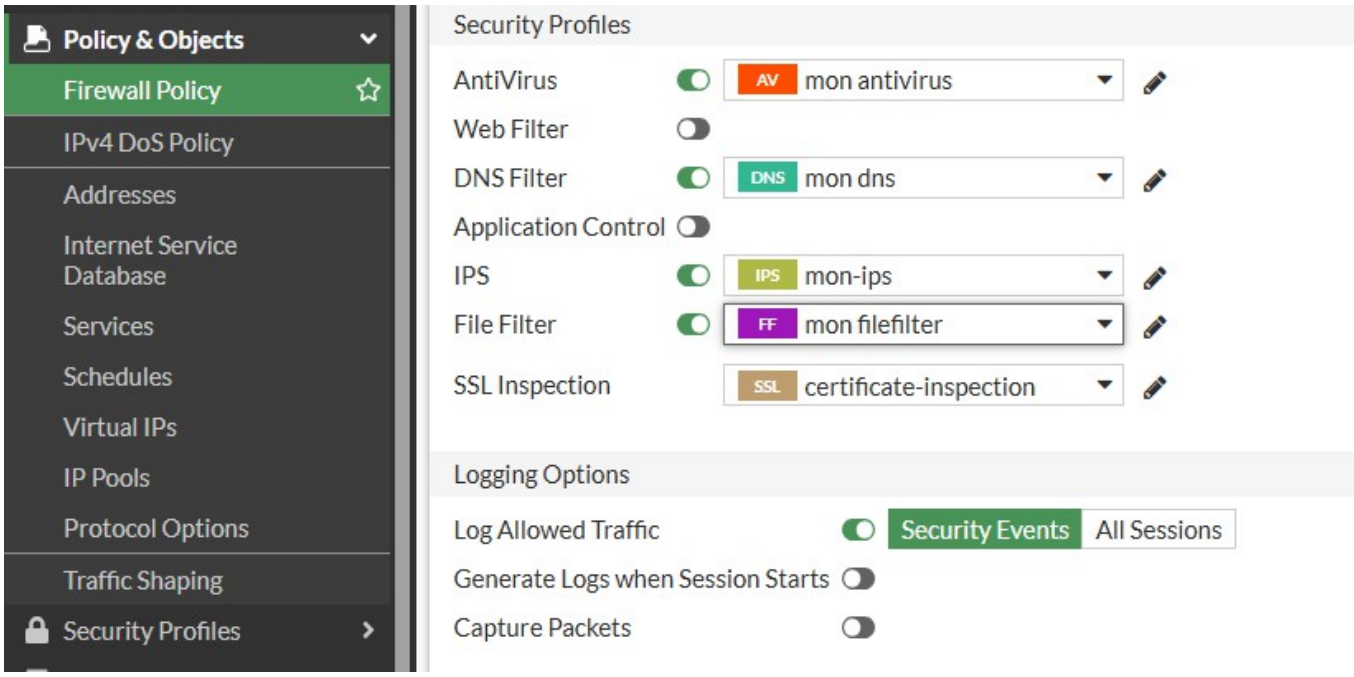


Figure 4.33 : Vérification des profils de sécurité appliqués

IV.8 Conclusion

Ce chapitre a été consacré à la configuration du pare-feu FortiGate, à travers l'analyse de différents scénarios d'évaluation des performances. Les résultats obtenus lors des tests se sont

révélés très satisfaisants. Toutefois, plusieurs fonctionnalités n'ont pas pu être testées en raison des limitations imposées par la version d'évaluation du pare-feu.

Pour explorer l'ensemble des fonctionnalités avancées (filtrage d'applications, VDOM, VPN IPsec/SSL, SD-WAN, inspection SSL, sandboxing, etc.), l'acquisition d'une licence complète permettrait de réaliser des tests plus représentatifs des usages réels en entreprise.

Conclusion générale

Ce projet de fin d'études nous a offert l'opportunité de mettre en œuvre, dans un environnement virtualisé, l'installation, la configuration et l'évaluation d'un pare-feu FortiGate, solution reconnue mondialement pour sa robustesse en matière de sécurité réseau. À travers l'utilisation d'outils professionnels tels que VMware Workstation, EVE-NG, FileZilla et WinSCP, nous avons construit une plateforme de test fidèle à un réseau réel, permettant d'expérimenter différentes politiques de sécurité.

Nous avons analysé en détail les fonctionnalités avancées de FortiGate, notamment les modules IPS, File Filter, antivirus, filtrage web, contrôle des applications, et DOS policy. Ces tests ont permis de valider l'efficacité de plusieurs services de sécurité, bien que certaines fonctionnalités n'aient pu être pleinement explorées en raison des limitations de la version d'évaluation. L'acquisition d'une licence complète représenterait une suite logique pour approfondir ces aspects.

Structuré autour d'un cheminement progressif, allant des principes fondamentaux de la cybersécurité à l'application pratique via FortiGate, ce travail nous a permis d'acquérir une vision globale et concrète de la sécurité réseau. Il a également renforcé nos compétences techniques tout en nous sensibilisant aux enjeux actuels de la cybersécurité en milieu professionnel.

En somme, ce projet constitue une base solide pour aborder les défis futurs liés à la gestion des infrastructures sécurisées et représente une étape importante dans notre parcours vers une carrière dans le domaine de la sécurité informatique.

Bibliographie

[1] David Décary-Hétu. Jun 08, 2020, article ”La cybercriminalité », https://www.crimrxiv.com/pub/zk9k26ba/release/1, consulté le 20/12/2024

[2] É. Filiol, Sécurité informatique : Principes et méthodes, Pearson Éducation, 2014

[3] Direction Générale de la Sécurité des Systèmes d’Information (DGSSI), Directive Nationale de la Sécurité des Systèmes d’Information (DNSSI), 2023. https://www.dgssi.gov.ma/fr/publications/directive-nationale-de-la-securite-des-systemes-dinformation-dnssi, consulté le 25/12/2024

[4] A. Bouzid, Support de cours : Sécurité des Réseaux Informatiques, Université Abdelhamid Mehri Constantine 2, Faculté NTIC, Oct. 2020.

[5] McGraw, Gary. "Software Security: Building Security In." Addison-Wesley Professional, 2006.

[6] Attaques et défenses dans les systèmes d'authentification des utilisateurs : une enquête. Journal of Network and Computer Applications, Volume 188, 15 août 2021.

[7] V. Bourdeix, Sécurité informatique sur le Web – Apprenez à sécuriser vos applications, Éditions ENI, 2021.

[8] ANSSI, "La sécurité physique des systèmes d'information," Agence nationale de la sécurité des systèmes d'information, 2014.

[9] Cobalt, "Common Network Security Vulnerabilities," Cobalt Blog, 2023.

[10] M. Lipp et al., "Meltdown: Reading Kernel Memory from User Space," in Proc. 27th USENIX Security Symposium, 2018, pp. 973–990.

[11] O. Kömmerling and M. G. Kuhn, "Design Principles for Tamper-Resistant Smartcard Processors," presented at. The USENIX Workshop on Smartcard Technology, Chicago, Illinois, USA, May 10–11, 1999

[12] OWASP Foundation, OWASP API Security Top 10 - 2023, Open Web Application Security Project, 2023.

[13] Kim Y., Kim I., Park N. (2014) Analysis of Cyber Attacks and Security Intelligence. In: Park J., Adeli H., Park N., Woungang I. (eds) Mobile, Ubiquitous, and Intelligent Computing. Lecture Notes in Electrical Engineering, vol 274. Springer, Berlin, Heidelberg.

[14] M. Hadnagy, Social Engineering: The Science of Human Hacking, 2nd ed., Wiley, 2018.

[15] N. Idoughi, A. Benzekri, and A. Bouabdallah, “Étude et classification des maliciels (malwares): Types, propagation et techniques d’obfuscation,” Revue des Nouvelles Technologies de l'Information, vol. B-8, pp. 67–80, 2015.

[16] Stallings, W. (2017). *Network security essentials: Applications and standards* (6th ed.). Pearson

[17] Jean Babtiste Favre, Firewall : architecture et déploiement, Creative Commons, 2006

[18] Patrick Ducrot-Sécurité Informatique-2009

[19] Xavier Tannier, « Se protéger sur Internet, Conseils pour la vie en ligne », édition Eyrolles, 2010.

[20] Ykhlef Hadjer, Hamzaoui Nesrine, « Etude et développement d’un firewall pour la sécurité d’un réseau informatique », thèse de licence, USDB, 2008/2009.

[22] Davis Chapman, « Firewalls – La sécurité sur Internet », edition O’Reilly, 1997.

[23] Xavier Tannier, « Se protéger sur Internet, Conseils pour la vie en ligne », édition Eyrolles, 2010.

[24] Cyrille Dufresnes. Pare-feu-Proxy-DMZ, 08/06/2008,, http://notionsinformatique.free.fr, consulté le 26/02/2025

[25] https://community.jisc.ac.uk/library/advisory-services/modes-firewall-operation, consulté le 11/03/2025

[26] Top 5 NGFW 2025. Enrico Bottos. 16 déc. 2024. https://www.nomios.com/news-blog/top-5-solutions-ngfw-2025/. consulté le 13/04/2025

[27] https://www.fortinet.com/, consulté le 5/04/2025

[28] https://www.vmware.com/ , consulté le 7/04/2025

[29] https://eve-ng.ru/, , consulté le 8/04/2025

[30] https://filezilla-project.org/, , consulté le 14/04/2025

Résumé

Dans le cadre de ce projet de fin d'études, nous avons entrepris un travail d'installation, de configuration et de test d'un pare-feu de nouvelle génération FortiGate, une solution de sécurité développée par l'entreprise Fortinet. FortiGate figure parmi les pare-feu réseau les plus largement déployés au niveau mondial. Il offre un large éventail de fonctionnalités avancées en matière de sécurité et de connectivité, réunies au sein d'une plateforme unifiée, centralisée via FortiGate Cloud.
L'objectif principal de ce projet était de mettre en place une plateforme de test virtuelle capable de simuler un environnement réseau réaliste, intégrant divers équipements, dans le but d'expérimenter et de valider plusieurs politiques de sécurité.
Les tests réalisés à l'aide d'une licence d'évaluation se sont révélés globalement très satisfaisants. Pour explorer l'ensemble des fonctionnalités avancées (filtrage d'applications et de contenus, VDOM, VPN IPsec/SSL, SD-WAN, inspection SSL, sandboxing, etc.), l'acquisition d'une licence complète permettrait de réaliser des tests plus représentatifs des usages réels en entreprise.
Ce projet nous a ainsi permis, d'une part, de renforcer nos compétences pratiques en sécurité informatique et en administration réseau, et d'autre part, de mieux appréhender les enjeux concrets de la cybersécurité.

Mots clés :
Cybersécurité, Attaque, Vulnérabilité, VMware, Eve-ng, Fortigate, NGFW, Pare-feu nouvelle génération, Proxy, DMZ, Filtrage

Abstract

As part of this final-year project, we undertook the installation, configuration, and testing of a next-generation firewall, FortiGate, a security solution developed by Fortinet. FortiGate is one of the most widely deployed network firewalls worldwide. It offers a broad range of advanced security and connectivity features, all integrated into a unified platform, centrally managed through FortiGate Cloud.
The main objective of this project was to set up a virtual testing platform capable of simulating a realistic network environment, integrating various devices, in order to experiment with and validate multiple security policies. The tests carried out using an evaluation license proved to be overall very satisfactory. However, to fully explore the set of advanced features (such as application and content filtering, VDOM, IPsec/SSL VPN, SD-WAN, SSL inspection, sandboxing, etc.), acquiring a full license would allow for more representative testing of real-world enterprise use cases.
This project has thus enabled us, on the one hand, to strengthen our practical skills in cybersecurity and network administration, and on the other hand, to gain a better understanding of the real-world challenges of cybersecurity.

Keywords : Cybersecurity, Attack, Vulnerability, VMware, Eve-ng, Fortigate, NGFW, Next generation Firewall, Proxy, DMZ, Filtering