

Mémoire de Master
En Informatique
Option :
Administration et sécurité des réseaux informatiques

Thème

**Sécurité réseaux à base d'un firewall software
FORTIGATE webfiltering (VMWARE)**

Présenté par :

Ghellaf warda & Lasmi Kenza

Soutenu le: 06 juillet 2022

Devant le jury composé de :

M. Sadi Mustapha

M.Bennai Yani-Athmane

M.Khenous Lachemi

M.Chekrid Mohamed

M.Bouakline Farouk

Encadrant

Co-Encadrant

Président

Examineur

Examineur

Année universitaire : 2021 / 2022

Remerciements

Nous tenons à remercier :

Le bon dieu de nous avoir donné la patience et la volonté pour accomplir ce travail.

Nos remerciements s'adressent également à :

Notre promoteur M.SADI Mustapha pour ses conseils, ses orientations pour nous avoir transmis les renseignements nécessaires à la réalisation de ce travail, ainsi que M.BENNAI Yani-Athmane qui nous a aidé et accompagné tout au long de cette expérience professionnelle.

Nous remercions également :

L'organisme d'accueil BMT tout particulièrement le chef de service informatique, Mr Benali, pour avoir mis à notre disposition la place de déroulement de notre stage.

Nous tenons également à remercier :

Les membres de jury, pour l'honneur qu'ils nous font en acceptant de juger, de lire et d'évaluer ce mémoire.

Enfin, nous remercions toutes personnes ayant contribué de près ou de loin à la réalisation de ce travail.

Dédicaces

Je tiens à dédier vivement ce modeste travail a mes très chers parents auxquels je dois ma réussite et auxquels je ne rendrai jamais assez .je leurs souhaite une longue vie,

Mon cher frère qui n'a pas cessé de me conseiller et encourager tout au long de mon parcours,

Ma petite sœur MERIEM,

Mes amis, tout particulièrement ma meilleure amie "Dihya" pour son soutien durant toutes ces années,

Et a toutes ma famille et mes proches.

M^{elle} LASMI Kenza

Je dédie ce travail à ma mère et mon père qui mon poussés être parmi les meilleurs et qui

M'ont encouragé et soutenue tous le long de ma vie,

Mon mari Madjid,

Ma petite sœur Fadoua,

Mes chères frères Bilal et Yakoub,

Mes amis,

Et a toutes ma famille et mes proches.

M^{me} GHELLAF Warda

Sommaire

Introduction Générale

CHAPITRE 1 : GENERALITES SUR LA SECURITE DANS LES RESEAUX INFORMATIQUE

Introduction

1.1 Réseau informatique	01
1.1.1 Définition d'un réseau informatique	01
1.1.2 Avantages d'un réseau informatique	01
1.1.3 Classification des réseaux	01
1.2. Le système d'information et la sécurité	02
1.2.1 Présentation	02
1.2.2 Les domaines d'intervention	03
1.3 Politiques de sécurité	04
1.3.1 Les différents types de politiques de sécurité	04
1.4. Les attaques informatiques	04
1.4.1 Présentation	04
1.4.2 Les différents types d'attaques	05
1.4.3 Les techniques d'attaques	05
1.5. Les mécanismes de détection et prévention d'attaques	07
1.5.1 Présentation Des IDS	07
1.5.2. Présentation des IPS	07
1.6. Les mécanismes de sécurité	07
1.6.1. La Cryptographie	08
1.6.2. La signature	08
1.6.3. Les Anti-virus	08
1.6.4. Le pare-feu (Firewall)	09
1.6.5. Réseaux privés virtuels (VPN)	09

Conclusion

CHAPITRE 2 : PRESENTATION DE L'ORGANISME D'ACCUEIL

Introduction

2.1. Présentation de l'organisme d'accueil	1	11
2.2 Situation géographique		11
2.3. Organigramme de l'entreprise		11
2.4. Département informatique		13
2.4.1 Les objectifs de la BMT		13
2.4.2 Les missions de la BMT		13
2.5. Les activités de la BMT		14
2.5.1. Opération de planification		14
2.5.2. Opération de manutention		14
2.5.3. Opération d'acconage		14
2.6. Infrastructure réseau de la BMT		15
2.7. Problématique		16
2.8. Objectifs		16

Conclusion

Sommaire

CHAPITRE 3 : FORTIGATE ET SECURITE RESEAUX

Introduction

3.1. Analyse technique préalable	17
3.2. Société Fortinet.....	18
3.3. L'approche Fortinet.....	18
3.4. Pare-feu de nouvelle génération (FortiGate)	19
3.5. Les solutions de Fortigate (UTM)	19
3.6. Avantages de l'utilisation d'une solution unifiée de gestion des menaces (UTM)	22
3.7. La Zone démilitarisée (DMZ)	22
3.7.1 La sécurité dans une DMZ.....	23
3.7.2 Architecture DMZ	23
3.8. Conception.....	24
3.8.1. Présentation de VMware Workstation.....	24
3.8.2. Présentation de FortiGate-VM.....	25
3.8.3. Présentation de Windows Server 2016.....	26

Conclusion

CHAPITRE 4 : CONTEXTE DE TRAVAIL ET IMPLEMENTATION

Introduction

4.1. Prérequis.....	28
4.2. Installation de Fortigate	29
4.2.1. Téléchargement de Fortigat VM.....	29
4.2.2. Installation de Fortigate sur VMWare Workstation	29
4.3. Configuration des interfaces de Fortigate	32
4.3.1. Configuration de l'interface LAN	32
4.3.2. Configuration de l'interface WAN.....	38
4.3.3. Configurer la DMZ sur le pare-feu FortiGate.....	49

Conclusion

Conclusion Générale

Bibliographie

LISTE DES ABREVIATIONS

BMT	Bejaia Méditerranéen Terminal
DHCP	Dynamic Host Configuration Protocol
DMZ	De-Militarized Zone
DNS	Domain Name System
EPB	Entreprise portuaire de Bejaia
FTP	file transfer protocol
HIPS	Host-based Intrusion Prevention System
HTTP	Hyper Text Transfert Protocol
IDS	Intrusion Detection System
IIS	Internet Information Servises
IP	internet protocol
IPS	Intrusion Prevention System
ISO	International Organization Standardization
KIPS	Kernel Intrusion Prevention System
LAN	Local Area Network
MAN	Métropolitain Area Network
MYSQL	My Structured Query Language
NAT	Network address translation
NIDS	Network Intrusion Detection System
NIPS	Network Intrusion Prevention System
PAN	Personale Area Network
PHP	Hypertext preprocessor
SMTP	Simple mail transfer protocol
TCP	Transmission Control Protocol
URL	Uniform Resource Locator
UTM	Unified threat management
VM	virtuel machine
VPN	Virtual Private Network
WAN	Wide Area Network
WIPS	Wireless Intrusion Prevention System
CLI	Command Line Interface

Listes des figures

<i>Figure 1.1: Les types de réseaux.....</i>	<i>02</i>
<i>Figure 1.2: Fonctionnement d'un VPN réseaux.....</i>	<i>10</i>
<i>Figure 2.1: Jointe venture de l'EPB et PORTEK.....</i>	<i>11</i>
<i>Figure 2.2 : Organigramme de l'entreprise.....</i>	<i>12</i>
<i>Figure 2.3 : Architecture réseau de la BMT.....</i>	<i>15</i>
<i>Figure 3.1 : De l'ancienne approche à la nouvelle.....</i>	<i>17</i>
<i>Figure 3.2 : Dispositif FortiGate.....</i>	<i>19</i>
<i>Figure 3.3 : Présentation des services FortiGate.....</i>	<i>20</i>
<i>Figure 3.4 : Schéma entre les réseaux à protéger.....</i>	<i>23</i>
<i>Figure 3.5 Interface d'accueil de VMware.....</i>	<i>25</i>
<i>Figure 3.6: Interface d'accueil de Fortigate.....</i>	<i>26</i>
<i>Figure 3.7 : Interface d'accueil de Windows serveur 2016.....</i>	<i>27</i>
<i>Figure 4.1 : Architecture réseau avec Fortigate.....</i>	<i>28</i>
<i>Figure 4.2 : Fichier de FortigateVm.....</i>	<i>29</i>
<i>Figure 4.3 : Importation de l'image Fortigate sur la VMWare</i>	<i>30</i>
<i>Figure 4.4 : Machine virtuelle de Fortigate.....</i>	<i>31</i>
<i>Figure 4.5 : Ecran de configuration de Fortigate</i>	<i>32</i>
<i>Figure 4.6 : Configuration de l'interface lan coté vmware.....</i>	<i>33</i>
<i>Figure 4.7 : Attribution du Switch virtuel au port 2.....</i>	<i>34</i>
<i>Figure 4.8 : écran de configuration de l'interface LAN.....</i>	<i>35</i>
<i>Figure 4.9 : Adresse de la machine physique.....</i>	<i>35</i>
<i>Figure 4.10 : Ping de la machine physique vers Fortigate</i>	<i>36</i>
<i>Figure 4.11 : Ping de Fortigate vers la machine physique</i>	<i>36</i>
<i>Figure 4.12 : Page d'identification de Fortigate.....</i>	<i>37</i>
<i>Figure 4.13 : Interface graphique du fortigate.....</i>	<i>37</i>
<i>Figure 4.14 : Configuration de l'interface web au bridged</i>	<i>38</i>
<i>Figure 4.15 : Attribuer un Switch virtuel au port 1.....</i>	<i>38</i>
<i>Figure 4.16 : écran de configuration de la carte réseau ETHERNET.....</i>	<i>39</i>
<i>Figure 4.17 : Configuration de l'interface WAN (DHCP).....</i>	<i>39</i>
<i>Figure 4.18 : Attribution switch 2 a l'interface LAN.....</i>	<i>40</i>
<i>Figure 4.19 : écran de configuration de la carte réseau du client.....</i>	<i>40</i>
<i>Figure 4.20 : Ping de Fortigate vers le client.....</i>	<i>41</i>
<i>Figure 4.21 : Ping de la machine client vers Fortigate.....</i>	<i>41</i>
<i>Figure 4.22 : Création de l'adresse objet.....</i>	<i>42</i>

Listes des figures

<i>Figure 4.23 : création de la politique LAN vers WAN</i>	43
<i>Figure 4.24 : Activer le NAT</i>	43
<i>Figure 4.25 : Stratégie du LAN TO WAN</i>	44
<i>Figure 4.26 : Tester le ping vers google</i>	44
<i>Figure 4.27 : Accéder au site internet (Linkedin)</i>	45
<i>Figure 4.28 : Créer un nouveau web Filter</i>	46
<i>Figure 4.29 : Créer un nouveau URL Filter</i>	46
<i>Figure 4.30 : Création d'URL Facebook</i>	47
<i>Figure 4.31 : Bloquer Facebook</i>	48
<i>Figure 4.32 : Local URL Filter block</i>	48
<i>Figure 4.33 : Machine virtuelle de Windows serveur 2016</i>	49
<i>Figure 4.34: Ecran de l'installation de Windows serveur</i>	50
<i>Figure 4.35 : Edition du système d'exploitation</i>	51
<i>Figure 4.36 : Type d'installation de Windows</i>	51
<i>Figure 4.37 :Emplacement de l'installation de Windows</i>	52
<i>Figure 4.38 : Ecran d'accueil de Windows serveur</i>	52
<i>Figure 4.39 : Création d'un site web</i>	53
<i>Figure 4.40 :Interface de notre site web</i>	54
<i>Figure4.41 : Configuration de l'interface DMZ</i>	54
<i>Figure 4.42 : Configuration de l'interface DMZ coté VMware</i>	55
<i>Figure 4.43 : Connecter le serveur au commutateur</i>	56
<i>Figure 4.44 : Ecran de configuration de la carte réseau du serveur</i>	56
<i>Figure 4.45:Création de l'adresse objet du PC LAN</i>	57
<i>Figure 4.46 : Création de l'adresse objet DMZ</i>	57
<i>Figure 4.47:Création de la politique LAN vers DMZ</i>	58
<i>Figure 4.48: Ping de la machine client vers le serveur</i>	59
<i>Figure 4.49 : Accueil de site web du serveur</i>	59

Introduction générale

Le développement du réseau internet, et de ses déclinaisons sous forme d'intranets et d'extranets, soulève des questions essentielles en matière de sécurité informatique.

L'accroissement des trafics en télécommunication révèlent les besoins grandissants d'échanges privés et professionnels. Ces transmissions de données imposent une ouverture des systèmes d'information vers l'extérieur, notamment vers internet. Celle-ci entraîne une certaine dépendance des entreprises et des personnes vis-à-vis des services qu'offre internet.

Cette ouverture et cette dépendance rendent l'entreprise vulnérable aux risques. C'est pour cela que la sécurité internet est devenue un sujet de recherche très sensible. Ces recherches ont permis le développement de certains dispositifs de sécurité comme les pare-feu de nouvelle génération (FortiGate), les antivirus et les systèmes de cryptographie pour protéger les systèmes informatiques.

FortiGate est un pare-feu de nouvelle génération permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers ou externe (internet). Ce système permet de filtrer les paquets de données échangés avec le réseau. Il s'agit ainsi d'une passerelle filtrant au minimum les interfaces réseau suivantes :

- Une interface pour le réseau à protéger (réseau interne LAN).
- Une interface pour le réseau externe WAN.
- Une interface DMZ.

Notre objectif dans ce travail est d'étudier les principaux mécanismes de sécurité utilisés par les entreprises dans le but de se protéger des menaces venant du réseau internet, et de proposer ainsi une solution de nouvelle génération pour notre organisme d'accueil. Notre mémoire s'articule donc autour de quatre principaux chapitres :

- Le premier chapitre est consacré aux généralités sur les réseaux et la sécurité informatique.
- Le deuxième chapitre décrit brièvement l'organisme d'accueil et présente la problématique de notre travail.
- Le troisième chapitre est focalisé sur les Firewalls (FortiGate), leurs principes de base et fonctionnement, ainsi que la zone démilitarisée (DMZ) et les outils de réalisation de notre solution.
- Le dernier chapitre présente la phase de réalisation : l'ensemble des configurations faites dans le cadre de l'implémentation de la solution proposée.

Nous terminons notre mémoire par une conclusion générale qui sert de synthèse à notre travail.

Introduction

La sécurité informatique est, de nos jours, devenue un problème majeur dans la gestion des réseaux d'entreprises, ainsi que pour les particuliers toujours plus nombreux à se connecter à Internet. Les réseaux sont toujours devant des menaces, et il y a de plus en plus de techniques pour les protéger mais, il y a aussi de plus en plus de techniques pour les attaquer.

L'objectif de ce chapitre est de présenter les concepts de base liés aux réseaux Informatiques ainsi qu'à la sécurité informatique.

1.1. Réseau informatique

1.1.1. Définition d'un réseau informatiques

Un réseau informatique est un ensemble d'équipements interconnectés qui délivrent des informations comme les serveurs ou bien qui reçoivent ou émettent des informations, tels que les ordinateurs, les terminaux bureautiques et les terminaux téléphoniques, etc. Un réseau peut être vu comme un ensemble de nœuds géographiquement distribués et reliés entre eux par des supports de transmission tels que le câble coaxial, la fibre optique ou la paire torsadée [1].

1.1.2. Avantages d'un réseau informatique

Un réseau informatique peut servir plusieurs objectifs différents [2] :

- Le partage de fichiers, d'applications et de ressources.
- La communication entre personnes (grâce au courrier électronique, la discussion en direct, etc.).
- La communication entre processus (entre des machines industrielles).
- La garantie de l'unicité de l'information (base de données).
- Les jeux vidéo multijoueurs.
- Les réseaux permettent aussi de standardiser les applications, telles que La messagerie électronique et les agendas de groupe qui permettent de communiquer plus efficacement et plus rapidement.

1.1.3. Classification des réseaux

Les réseaux peuvent être classés en fonction de l'éloignement maximal entre ses stations.

Nous distinguons généralement les catégories de réseaux suivantes [3] :

- a. **Les réseaux PAN** : Les réseaux personnels, ou PAN (Personale Area Network), Interconnectent sur quelques mètres des équipements personnels d'un même utilisateur.

- b. Les réseaux LAN :** Local Area Network ou réseau local, permettent de connecter deux à plusieurs centaines de machines à l'intérieure d'une même zone. Il s'agit de la plupart des réseaux informatiques présents dans les entreprises.
- c. Les réseaux MAN :** Métropolitain Area Network, il s'agit d'un réseau dont la couverture s'étale sur une ville. Le principe est de relier les différents réseaux locaux, mais les normes des transmissions sont différentes. Un MAN est donc une série de réseaux locaux interconnectés à l'échelle d'une ville.
- d. Les réseaux WAN :** Wide Area Network ou réseau de grande taille, il interconnecte des réseaux MAN pour assurer une couverture et une interconnexion au niveau d'un pays, Voir à travers le monde. Ce type de réseau utilise les satellites pour certaines Interconnexions. Le WAN le plus célèbre est le réseau public Internet, dont le nom provient de cette qualité : Inter Networking, ou interconnexion de réseau.

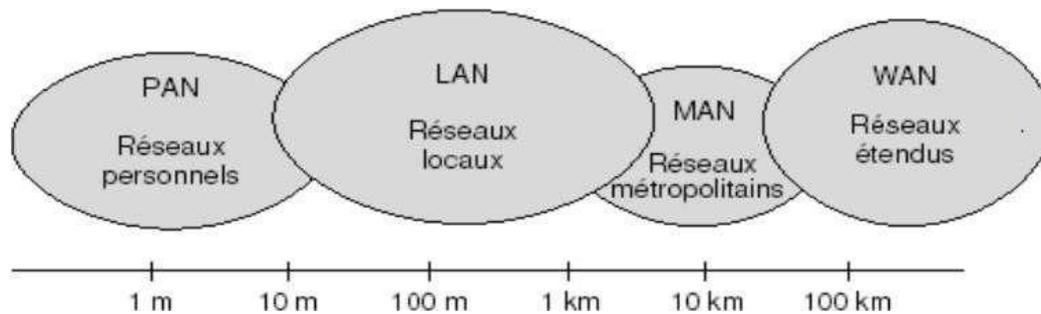


Figure 1.1: Les types de réseaux

1.2. Le système d'information et la sécurité

1.2.1. Présentation

Le système d'information représente l'ensemble des données de l'entreprise ainsi que ses infrastructures matérielles et logicielles. Il représente un patrimoine essentiel de l'entreprise, qu'il convient de protéger.

La sécurité informatique est l'ensemble des moyens techniques, organisationnels, juridiques et humains qui visent à s'assurer que les ressources matérielles et logicielles d'une organisation soient uniquement utilisées dans le cadre prévu.

La sécurité informatique vise généralement cinq principaux objectifs [4] :

- **L'intégrité :** qui garantit que les données n'ont pas été modifiées, altérées ou détruites durant la communication tant de façon intentionnelle qu'accidentelle.

- **La confidentialité** : qui consiste à rendre l'information inintelligible à d'autres personnes, autre que les seuls acteurs de la transaction.
- **La disponibilité** : l'information sur le système doit être toujours disponible aux personnes autorisées.
- **La non-répudiation** : de l'information qui est la garantie qu'aucun des correspondants ne pourra nier la transaction.
- **L'authentification** : qui consiste à assurer l'identité d'un utilisateur, c'est-à-dire à garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être.

1.2.2. Les domaines d'intervention

Toutes les sphères d'activité de l'informatique sont concernées par la sécurité d'un système d'information.

En fonction de son domaine d'application, la sécurité informatique se décline en [5] :

- **Sécurité physique** : concerne tous les aspects liés à la maîtrise des systèmes et de l'environnement dans lesquels ils se situent.
 - La protection des sources énergétiques (alimentation).
 - La protection de l'environnement (incendie, température, humidité).
 - La protection des accès (protection physique des équipements, infrastructure câblée, redondance des alimentation énergétiques).
 - La sûreté de fonctionnement et la fiabilité des matériels (composants, câbles).
- **Sécurité de l'exploitation** : Concerne tous ce qui touche au bon fonctionnement des systèmes. Cela comprend la mise en place d'outils et de procédures relatifs aux méthodologies d'exploitation, de maintenance, de test, de diagnostic et de mise à jour.

En particulier, la sécurité de l'exploitation dépend fortement de son degré d'industrialisation.

- **La sécurité logique** : fait référence à la réalisation de mécanismes de sécurité par logiciel. Elle repose sur la mise en œuvre d'un système **de Contrôle d'accès logique** s'appuyant sur un service **d'authentification, d'identification et d'autorisation**. Elle repose également sur :
 - Les dispositifs mis en place pour garantir la confidentialité dont la cryptographie.
 - Une gestion efficace des mots de passe et des procédures d'authentification.
 - Des mesures antivirus et de sauvegarde des informations sensibles.
- **Sécurité applicative** : comprend un développement pertinent de solutions logicielles ainsi que leur intégration et exécution harmonieuses dans des environnements opérationnels.
- **Sécurité des télécommunications** : Cela implique la réalisation d'une infrastructure réseau sécurisée au niveau des accès, des protocoles de communication, des systèmes d'exploitation et des équipements.

1.3. Politique de sécurité

Une politique de sécurité est perçue comme une réglementation particulière dont l'objectif est de décrire la façon de gérer, protéger et diffuser les informations et les autres ressources sensibles au sein d'un système informatique [5].

1.3.1. Les différents types de politiques de sécurité

Une politique de sécurité peut être trop permissive ou au contraire trop restrictive. Dans le premier cas, elle risque de présenter une faiblesse de sécurité par son côté laxiste. Dans le second, elle peut devenir inapplicable du fait de règles trop strictes.

Toutes déviations de la politique de sécurité fait l'objet d'une revue spécifique afin de corriger la faiblesse de sécurité engendrée et les exceptions associées.

La politique de sécurité a pour rôle de [5] :

- Définir le cadre d'utilisation des ressources du système d'information.
- Identifier les techniques de sécurisation à mettre en œuvre dans les différents services de l'organisation.
- Sensibiliser les utilisateurs à la sécurité informatique.

Une politique de sécurité réseau couvre les éléments suivants [5] :

- **Sécurité de l'infrastructure** : couvre la sécurité logique et physique des équipements et des connexions réseau, aussi bien internes que celles fournies par des fournisseurs réseau.
- **Sécurité des accès** : couvre la sécurité logique des accès locaux et distants aux ressources de l'entreprise, ainsi que la gestion des utilisateurs et de leurs droits d'accès au système d'informations de l'entreprise.
- **Sécurité du réseau Intranet face à Internet ou aux autres parties** : couvre la sécurité logique des accès aux ressources de l'entreprise (Intranet) et l'accès aux ressources extérieures (Extranet).

Pour résumer, la définition d'une politique de sécurité réseau vise tout à la fois à définir les besoins de sécurité de l'entreprise, à élaborer des stratégies de sécurité afin de protéger les biens les plus critiques et à définir le référentiel des contrôles de sécurité.

1.4. Attaques sur la sécurité informatiques

1.4.1. Présentation

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque. Sur Internet, des attaques ont lieu en permanence, à raison de plusieurs attaques par minute sur chaque machine connectée. Ces attaques sont pour la plupart lancées automatiquement à partir de machines infectées (par des virus, chevaux de Troie, etc.), à

l'insu de leur propriétaire. Plus rarement il s'agit de l'action directe de **pirates informatiques**.

Afin de contrer ces attaques, il est indispensable de connaître les principaux types d'attaques pour mieux s'y préparer.

1.4.2. Les différents types d'attaque

Les attaques peuvent être regroupées en trois familles différentes [6] :

- **Les attaques directes**

C'est la plus simple des attaques. Le hacker attaque directement sa victime à partir de son ordinateur. En effet, les programmes de hack qu'il utilise ne sont que faiblement paramétrables, et un grand nombre de ces logiciels envoient directement les paquets à la victime.

- **Les attaques indirectes par rebond**

Cette attaque est très prisée des hackers, le rebond à deux avantages principaux :

- Masquer l'identité (l'adresse IP) d'un hacker.
- Utiliser les ressources de l'ordinateur intermédiaire car, il est plus puissant (CPU, bande passante) pour réaliser son attaque.

Le principe, en lui-même, est simple : les paquets d'attaque sont envoyés à l'ordinateur intermédiaire qui répercute l'attaque vers la victime. D'où le terme de rebond.

- **Les attaques indirectes par réponse**

Cette attaque est un dérivée de l'attaque par rebond. Elle offre les mêmes avantages du point de vue du hacker, à la différence d'envoyer une requête, c'est la réponse à cette requête qui va être envoyée à l'ordinateur victime.

1.4.3. Les techniques d'attaques

a. Techniques d'attaque par messagerie

En dehors des nombreux programmes malveillants qui se propagent par la messagerie électronique, il existe des attaques spécifiques [7] :

- Le pourriel (spam en anglais) : un courrier électronique non sollicité, la plupart du temps de la publicité. Ils encombrant le réseau, et font perdre du temps à leurs destinataires.
- L'hameçonnage (phishing en anglais) : un courrier électronique dans lequel l'expéditeur se fait généralement passer pour un organisme financier et demande au destinataire de fournir des informations confidentielles.

- Le canular informatique (hoax en anglais) : un courrier électronique incitant généralement le destinataire à retransmettre le message à ses contacts sous divers prétextes. Ils encombrant le réseau, et font perdre du temps à leurs destinataires. Dans certains cas, ils incitent l'utilisateur à effectuer des manipulations dangereuses sur son poste (suppression d'un fichier prétendument lié à un virus par exemple).

b. Attaques sur le réseau

- Le sniffing : technique permettant de récupérer toutes les informations transitant sur un réseau (on utilise pour cela un logiciel sniffer). Elle est généralement utilisée pour récupérer les mots de passe des applications qui ne chiffrent pas leurs communications, et pour identifier les machines qui communiquent sur le réseau [7].
- La mystification (spoofing en anglais) : technique consistant à prendre l'identité d'une autre personne ou d'une autre machine. Elle est généralement utilisée pour récupérer des informations sensibles que l'on ne pourrait pas avoir autrement [7].
- Le déni de service (en anglais denial of service) : technique visant à générer des arrêts de service, et ainsi d'empêcher le bon fonctionnement d'un système [7].

Et d'autres techniques moins utilisées :

- Hijacking
- Attaque de l'homme du milieu (MITM)
- Fragments attacks
- Tiny Fragments
- Fragment Overlapping
- TCP Session Hijacking

c. Attaques sur les mots de passe

Les attaques sur les mots de passe peuvent consister à faire de nombreux essais jusqu'à trouver le bon mot de passe.

Dans ce cadre, notons les deux méthodes suivantes [7]:

- **L'attaque par dictionnaire** : le mot testé est pris dans une liste prédéfinie contenant les mots de passe les plus courants et aussi des variantes de ceux-ci (à l'envers, avec un chiffre à la fin, etc.). Ces listes sont généralement dans toutes les langues les plus utilisées, contiennent des mots existants, ou des diminutifs (comme "powa" pour "power", ou "G0d" pour "god").
- **L'attaque par force brute** : on appelle ainsi (brut force cracking ,ou parfois attaque exhaustive)le cassage d'un mot de passe en testant tous les mots de passe possibles.

On peut noter qu'il existe d'autres types d'attaques, souvent moins connues car, nécessitant des compétences très pointues.

1.5 Les mécanismes de détection et prévention d'attaques

1.5.1 Présentation des IDS

Un **système de détection d'intrusion** (ou IDS : *Intrusion Detection System*) est un mécanisme écoutant le trafic réseau de manière furtive afin de repérer des activités anormales ou suspectes et permettant ainsi d'avoir une action de prévention sur les risques d'intrusion. Il existe deux niveaux d'IDS [8] : les IDS systèmes et les IDS réseaux.

➤ **Les IDS systèmes (Host IDS)**

Un système de détection d'intrusion basé sur l'hôte est une application surveillant un ordinateur ou un réseau pour détecter toute activité suspecte, qui peut inclure des intrusions par des acteurs externes ainsi qu'une mauvaise utilisation des ressources ou des données par des acteurs internes [8].

➤ **Les IDS réseaux (network IDS)**

Un système de détection d'intrusion réseau (NIDS) surveille les paquets entrant et sortant d'un réseau. Il peut surveiller tout le trafic, ou juste une partie, pour détecter les menaces de sécurité [8].

En cas de détection d'intrusion, des alertes peuvent être envoyées.

1.5.2 Présentation des IPS

Définition

Un **système de prévention d'intrusion** (ou IPS, *Intrusion Prevention System*) est un outil des spécialistes en sécurité des systèmes d'information, similaire aux IDS, permettant de détecter une attaque sur le système surveillé et de mettre en place des mécanismes de défense permettant de mitiger l'attaque [8], parmi les types D'IPS on trouve :

➤ **Système de prévention des intrusions par le réseau**

Les NIPS (Network Intrusion Prevention System) sont des IPS permettant de surveiller le trafic réseau, ils peuvent prendre des mesures telles que terminer une session TCP. Une déclinaison en WIPS (Wireless Intrusion Prevention System) est parfois utilisée pour évoquer la protection des réseaux sans-fil [7].

➤ **Système de prévention des intrusions basées sur l'hôte**

Les HIPS (Host-based Intrusion Prevention System) sont des IPS permettant de surveiller le poste de travail à travers différentes techniques ils surveillent les processus, les drivers, etc. Encas de détection de processus suspect, le HIPS peut le tuer pour mettre fin à ses agissements. Il existe aussi les KIPS (Kernel Intrusion Prevention System) qui permettent de détecter toutes tentatives d'intrusion au niveau du noyau mais, ils sont moins utilisés [7].

1.6. Mécanismes de sécurité

1.6.1. Cryptographie

La cryptographie est une science permettant de convertir des informations « en clair » en informations chfrées, c'est-à-dire non compréhensibles, puis à partir de ces informations codées de restituer les informations originales. Il existe deux grandes familles d'algorithmes cryptographiques à base de clef [7].

➤ **Cryptage symétrique**

Dans la cryptographie symétrique, les clés de chiffrement et de déchiffrement sont identiques : c'est la clé secrète, l'émetteur et le récepteur doivent posséder et utiliser la même clé secrète pour rendre confidentielles des données et pour pouvoir les comprendre [7].

➤ **Cryptage asymétrique**

Un système de chiffrement asymétrique est basé sur l'usage d'un couple unique de deux clés complémentaires (clé publique, clé privée), calculées l'une par rapport à l'autre. La cryptographie asymétrique utilise cette paire de clés pour le chiffrement et le déchiffrement. La clé publique est distribuée librement, et la clé privée, quant à elle, n'est jamais distribuée et doit être gardée secrète [7].

1.6.2. Signature numérique

La signature numérique : L'une des utilisations de la cryptographie à clé publique est qu'elle permet l'établissement des signatures numériques. Ces dernières offrent au destinataire la possibilité de vérifier l'authenticité de l'expéditeur (origine exacte).

Ces signatures sont liées aux informations qu'elles attestent, elles sont donc difficiles à falsifier. Elles apportent aussi l'authentification et l'identification des parties concernées et la non-répudiation en cas de désaveu de la part de l'expéditeur.

Le principe de la signature numérique est qu'elle est le résultat du cryptage du document et d'autres informations concernant l'expéditeur avec sa clé privée, affirmant ainsi son authenticité [7].

1.6.3. Les Anti-virus

Les antivirus sont des programmes de sécurité capables de détecter la présence de virus sur un ordinateur, ainsi que de nettoyer celui-ci dans la mesure du possible si jamais un ou plusieurs virus sont trouvés. Nettoyer signifie supprimer le virus du fichier sans l'endommager. Mais, parfois ce nettoyage simple n'est pas possible [8].

1.6.4. Le pare-feu (Firewall)

Un pare-feu [9], (appelé aussi coupe-feu, garde-barrière, barrière de sécurité, ou encore firewall en anglais), est un logiciel et/ou un matériel, permettant de faire respecter la politique de Sécurité du réseau, celle-ci définissant quels sont les types de communications autorisées sur ce réseau informatique [9].

1.6.4.1. Principe et fonctionnement

Un système pare-feu contient un ensemble des règles prédéfinies permettant [9] :

- D'autoriser la connexion (allow) ;
- De bloquer la connexion (deny) ;
- De rejeter la demande de connexion sans avertir l'émetteur (drop).

L'ensemble de ces règles permettent de mettre en œuvre une méthode de filtrage dépendant de la politique de sécurité adoptée par l'entreprise.

On distingue habituellement deux types de politiques de sécurité permettant :

- 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.

La première méthode est sans nul doute la plus sûre mais, elle impose toutefois une définition précise et contraignante des besoins en communication.

1.6.5. Réseaux privés virtuels (VPN)

Un VPN (Virtual Private Network en anglais) permet de canaliser un trafic sécurisé d'un point à un autre sur des réseaux généralement hostiles (internet par exemple) [8].

1.6.5.1. Fonctionnement d'un VPN

Un VPN repose sur un protocole appelé **protocole de tunnelisation** (tunneling). c'est-à-dire un protocole permettant aux données passant d'une extrémité du VPN à l'autre d'être sécurisées par des algorithmes de cryptographie [9].

L'expression **tunnel chiffré** est utilisée pour symboliser le fait qu'entre l'entrée et la sortie du VPN, les données sont chiffrées (cryptées) et donc incompréhensibles pour toute personne située entre les deux extrémités du VPN, comme si les données passaient dans un tunnel.

Dans le cas d'un VPN établi entre deux machines, on appelle **client VPN** l'élément permettant de chiffrer et de déchiffrer les données du côté utilisateur (client), et **serveur VPN (serveur d'accès distant)** l'élément chiffrant et déchiffrant les données du côté de l'organisation [9].

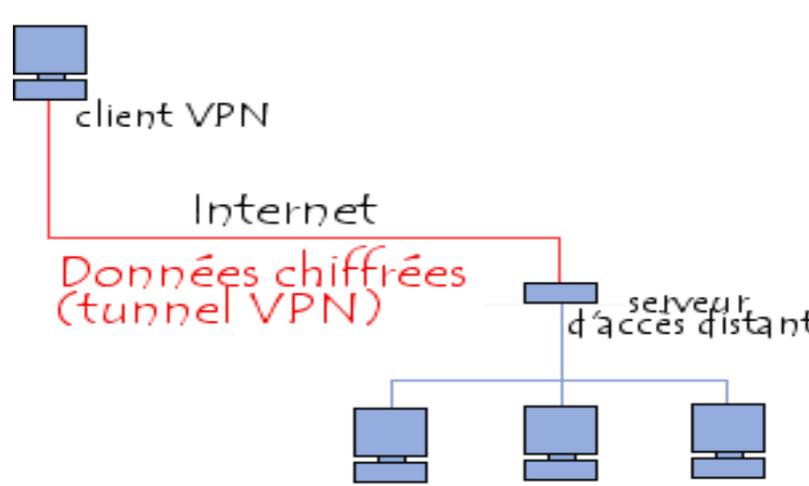


Figure 1.2: Fonctionnement d'un VPN

De cette façon, lorsqu'un utilisateur a besoin d'accéder au réseaux privé virtuel, sa requête va être transmise en clair au système passerelle, qui va se connecter au réseau distant par l'intermédiaire d'une infrastructure de réseau public puis, va transmettre la requête de façon chiffrée.

L'ordinateur distant va alors fournir les données au serveur VPN de son réseau local qui va transmettre la réponse de façon chiffrée.

A la réception sur le client VPN de l'utilisateur, les données seront déchiffrées, puis transmises à l'utilisateur.

Conclusion

Dans ce chapitre, nous avons défini quelques notions fondamentales sur les réseaux Informatiques et les différents types d'attaque, ainsi que les outils à utiliser et la stratégie à entreprendre afin de mettre en place une politique de sécurité.

Dans le prochain chapitre, nous allons présenter l'organisme d'accueil.

Introduction

Dans ce chapitre, nous allons présenter l'entreprise dans laquelle nous avons effectué notre stage pour la réalisation de notre projet de fin de cycle. Nous commençons d'abord par une brève présentation de la BMT Bejaia, puis nous introduisons la structure générale de son organisation avec ses différentes directions et en particulier sa direction informatique, ainsi que ces objectifs. Ensuite, nous ferons le point sur la problématique posée et la solution proposée.

2.1. Présentation de l'organisme d'accueil

BMT (Bejaia Méditerranéen Terminal) est une jointe venture entre l'Entreprise portuaire de Bejaia (EPB) et Portek Systems & Equipment. EPB est l'autorité portuaire qui gère le port de Bejaia. PORTEK Systems and Equipment, filiale du groupe PORTEK, est un opérateur de Terminaux à conteneurs présent dans plusieurs ports dans le monde, spécialisé dans les équipements portuaires.

L'activité principale de BMT est la gestion et l'exploitation du terminal à conteneurs. Sa mission principale est de traiter dans les meilleures conditions de délais, de coûts et de sécurité, l'ensemble des opérations qui ont rapport avec le conteneur. Pour ce faire, elle s'est dotée d'équipements performants et de systèmes informatiques pour le support de la logistique du conteneur afin d'offrir des services de qualité, efficaces et fiables pour assurer une satisfaction totale des clients [10].

2.2. Situation géographique

L'entreprise BMT se situe au niveau du port de Bejaia, ce dernier est implanté au centre du Nord-Est du pays et jouit d'une situation géographique stratégique. Elle se trouve à proximité de la gare ferroviaire, à quelques minutes de l'aéroport de Bejaia et elle est reliée au réseau routier national qui facilite le transport des marchandises conteneurisées de toute nature vers l'ensemble des régions du pays [10].

2.3. L'organigramme de l'entreprise



Figure 2.1: Jointe venture de l'EPB et PORTEK

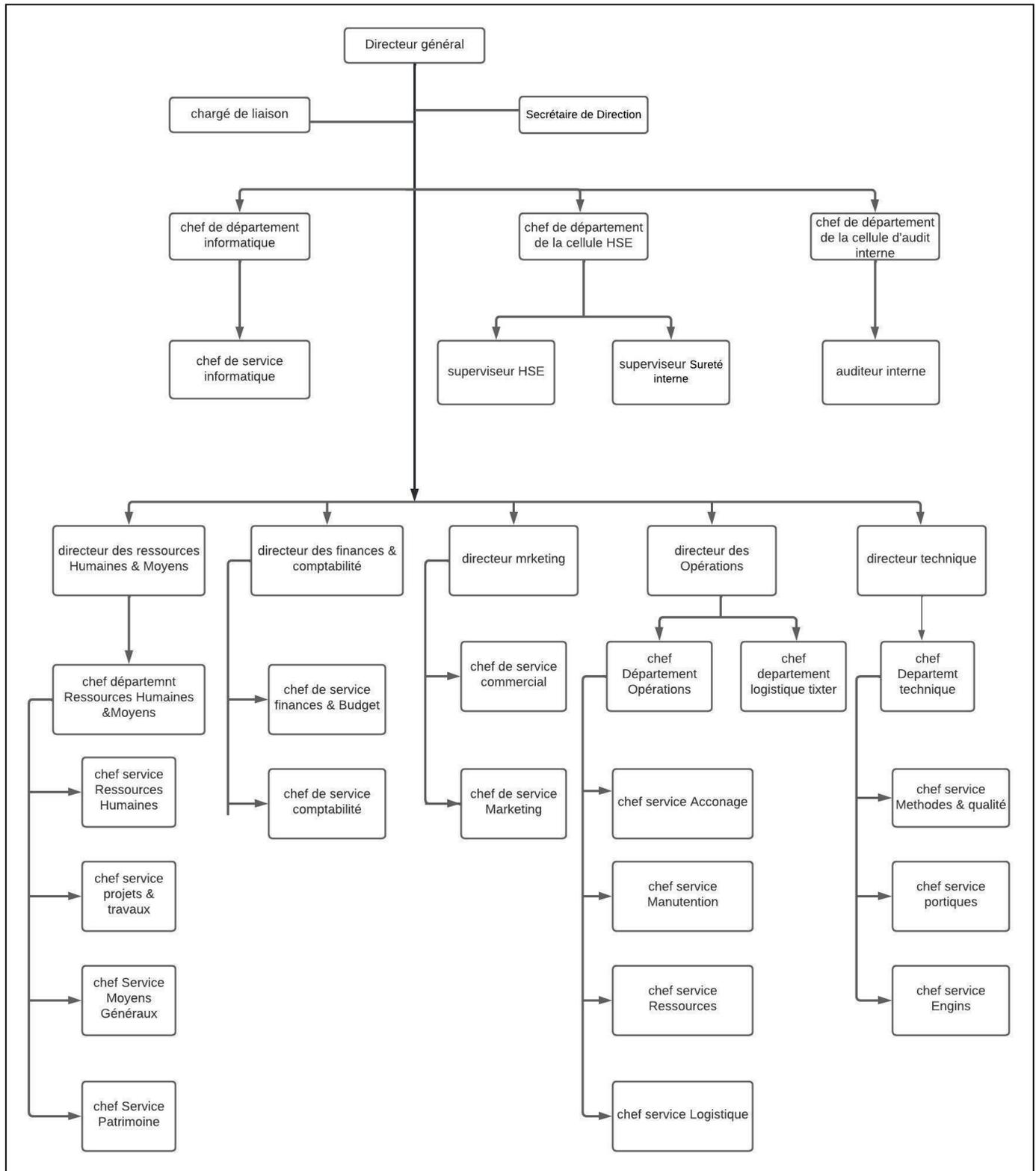


Figure2.2 : Organigramme de l'entreprise

2.4. Département informatique

C'est un service qui appartient à la direction générale, ses principales fonctions sont :

- Suivi des applications de gestion.
- La maintenance du parc informatique de l'entreprise.
- Audit et amélioration du système d'information.
- Sauvegarde et contrôle des données de l'entreprise.
- Développement de nouvelles applications aux différentes structures.

2.4.1. Objectifs de la BMT

- ✓ Faire du terminal à conteneurs de la BMT une infrastructure moderne tout en répondant aux exigences les plus élevées en matière de qualité dans le traitement des conteneurs.
- ✓ Mettre à sa disposition une nouvelle technologie dans le traitement des conteneurs en vue d'assurer :
 - Gain de productivité ;
 - Réduction des coûts d'escale ;
 - Fiabilité de l'information ;
 - Meilleur service ;
 - Sauvegarder la marchandise des clients ;
 - Faire face aux concurrences nationales et internationales ;
 - Propulser le terminal au stade international ;
 - Gagner des parts du marché.
- ✓ Faire passer de 20 à 30 conteneurs à l'heure.
- ✓ Créer et gérer un centre de formation.

2.4.2. Missions de la BMT

BMT a comme activité principale le suivi, la gestion et l'exploitation du terminal à conteneur. Elle a pour missions principales :

- Traiter dans les meilleures conditions de délais, de coûts et de sécurité, l'ensemble des navires porte-conteneurs et des conteneurs,
- Manutention sur navire (aussi bien le chargement et le déchargement) des conteneurs et leurs entreposages dans les zones de stockage.
- Fournir les prestations de service d'acconage sur les aires spécialisées ainsi que leurs livraisons.

- Déchargement des céréales selon la capacité de la BMT.

Pour ce faire, il est doté d'équipements performants et du système informatisé « CTMS » liés à la logistique permettant à la fois d'offrir avec efficacité et fiabilité, des services de qualité ainsi que de satisfaire les différents besoins des clients.

2.5. Activités de la BMT

Bejaia Méditerranéen Terminal reçoit annuellement un grand nombre de navires aux quels assure les opérations de planifications, de manutention et d'aconage avec un suivi et une traçabilité des opérations.

2.5.1. Opération de planification

- ✓ Planification des escales : programmation des accostages et des postes à quai.
- ✓ Planification déchargement/chargement.
- ✓ Planification du parc à conteneurs (visite, dépotage, enlèvement et restitution des conteneurs vides au parc).
- ✓ Planification des ressources : Equipes et moyens matériels.

2.5.2. Opération de manutention

Elle comprend les opérations :

- ✓ D'embarquement, de débarquement des conteneurs.
- ✓ De réception des navires porte-conteneurs.

La manutention est opérationnelle de jour comme de nuit, répartie en deux shifts de 07h00 à 13h00 et de 13h00 à 19h00 avec un troisième shift « over time » optionnel qui s'étale jusqu'à 07h00 du matin.

2.5.3. Opération d'aconage

- Transfert des conteneurs vers les zones d'entreposage.
- Transfert des conteneurs frigorifiques vers les zones <<reefers>>.
- Suivi des visites du conteneur par les services concernés.

- Chargement de position des conteneurs.
- Suivi des livraisons et des dépotages.
- Suivi des restitutions et des mises à quai.
- Mise à disposition des conteneurs vides pour empotage.

2.6. Infrastructure réseau de la BMT

La cartographie ci-dessous montre l'architecture réseau de la BMT :

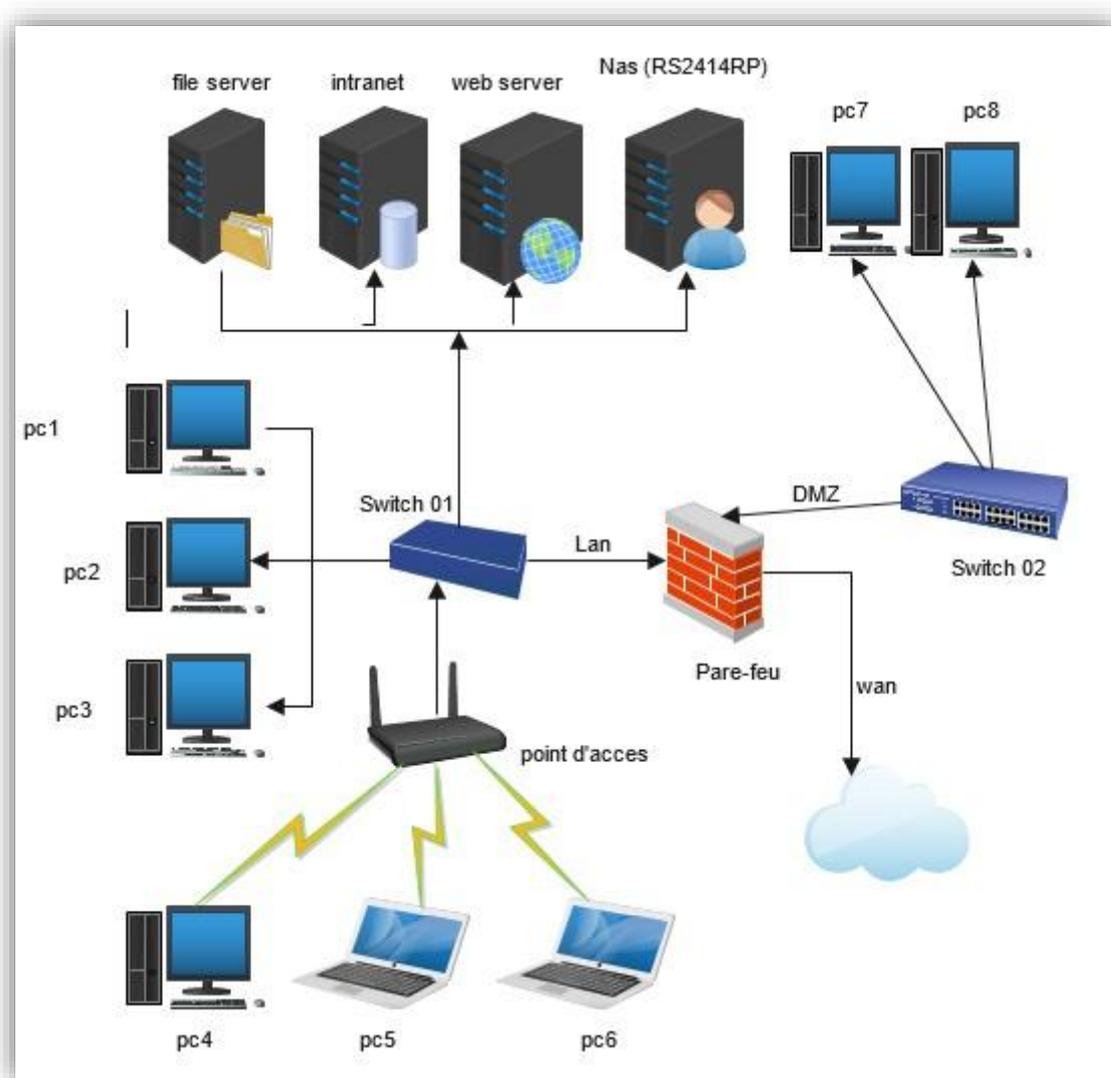


Figure 2.3 : Architecture réseau de la BMT

2.7. Problématique

Le réseau BMT comme n'importe quel autre réseau n'est pas sans faille en terme de sécurité réseau, à cause entre autres du nombre élevé de ses utilisateurs qui viennent de partout dans le monde.

Au cours de nos visites au sein de l'entreprise, nous avons constaté des anomalies au niveau de la sécurisation du réseau de l'entreprise, nous les énumérons comme suit :

- Absence d'un Fortigate qui doit filtrer les connexions entrantes et sortantes de l'infrastructure et bloquer les accès non autorisés.
- Absence d'une zone démilitarisée (DMZ) qui doit être accessibles de l'extérieur.

2.8. Objectifs

Le projet est de créer une passerelle entre le réseau interne et le réseau internet. La finalité est de pouvoir déployer la solution dans toutes les structures de nos problématiques au niveau de l'entreprise BMT. C'est dans ce but qu'il nous a été demandé de mettre en place un firewall pour pouvoir gérer la connexion sortante à partir du réseau local, protéger le réseau interne des intrusions venant de l'extérieur, et surveiller/tracer le trafic entre le réseau local et internet.

Conclusion

A travers ce chapitre, nous avons introduit l'organisme d'accueil de BMT. Cette présentation nous a permis de mieux comprendre sa structure, ainsi que le rôle et les missions du département informatique, tout en dégageant les failles identifiées et citant les solutions proposées.

Dans le chapitre suivant, nous allons présenter les principaux outils que nous avons utilisé dans notre solution proposée.

Introduction

Même si la sécurité d'un ordinateur et les informations qu'il contient sont bien assurées, cela reste insuffisant lorsqu'on veut communiquer avec d'autres ordinateurs que ce soit à partir d'un réseau local ou d'un réseau externe tel que internet.

Pour une sécurité accrue de notre système, nous devons augmenter le niveau de sécurité en utilisant un pare-feu de nouvelle génération (Fortigate).

3.1. Analyse technique préalable

La solution de sécurité traditionnelle consiste à avoir plusieurs mécanismes de sécurité hétérogènes au sein d'une entreprise. Avant l'apparition du concept de « UTM », les entreprises étaient obligées d'avoir un équipement et une technologie différentes pour chaque type de sécurité à mettre en place, par exemple un pare-feu (firewall), un antivirus et un anti spam, etc. L'avantage de cette méthode traditionnelle est qu'elle permet de garantir une sécurité renforcée, l'inconvénient est une utilisation élevée des ressources, et donc une augmentation de l'utilisation d'énergie et de consommation d'espace. En plus de cela, elle nécessite une formation des ingénieurs sur des technologies différentes, ce qui coûte beaucoup d'argent.

Il faut donc trouver une solution adaptée aux moyens et à l'environnement de l'entreprise.

L'approche Fortinet est venue avec un concept qui s'appelle UTM, qui consiste à mettre en place l'ensemble des mécanismes de sécurité nécessaires dans un seul boîtier.

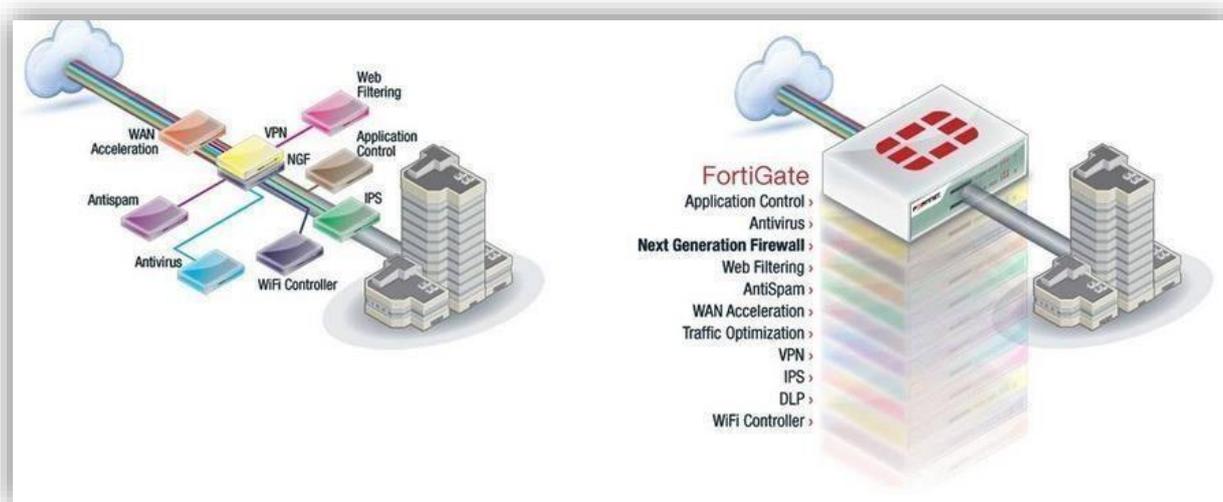


Figure 3.1 : De l'ancienne approche à la nouvelle

3.2. Société Fortinet

Fortinet a été créée en 2000 par les frères Ken et Michael, elle est une multinationale américaine dont le siège social se situe à Sunnyvale (Californie). Elle conçoit et commercialise, entre autres, des logiciels, équipements (Appliances) et services de cyber sécurité tels que des pare-feu, anti-virus, systèmes de prévention d'intrusion et de sécurité des terminaux. Elle occupe le quatrième rang mondial des acteurs de la sécurité réseau quant au chiffre d'affaires.

Fortinet fournit des solutions de sécurité haute performance qui protègent les réseaux informatiques, les utilisateurs et les données contre des menaces en évolution permanente. Sa gamme étendue de solutions de sécurité et de plateformes de gestion centralisées permet de consolider la sécurité et de simplifier son infrastructure [11].

3.3. L'approche Fortinet

Fortinet s'est spécialisé sur le marché des UTM, équipements intégrant plusieurs fonctionnalités en une seule Appliance associée à une console unique de management et reporting. Cette approche procure plusieurs avantages, dont notamment [11] :

- Optimiser les ressources.
- Déploiements, administration et exploitation simplifiés.
- Réduire le nombre d'équipements hétérogènes.
- Modules de sécurité intégrés.
- Sécurité avancée en profondeur.
- Mises à jour automatiques et constante pour plusieurs fonctionnalités en une fois.
- Support unique.
- Mises à niveau des compétences simplifiées.
- Coûts d'acquisition et de maintenance réduits.
- Retour sur investissement rapide, coût total de possession réduit.

En termes de sécurité, cette approche permet d'avoir des analyses multi-niveaux complémentaires notamment au niveau du contenu des applications, l'ensemble étant intégré.

3.4. Pare-feu de nouvelle génération (FortiGate)

Le pare-feu de nouvelle génération Fortigate utilise des processeurs de sécurité spécialement créés, ainsi que des services de renseignements sur les menaces des laboratoires Fortiguard pour offrir une protection de premier ordre et des performances élevées. En plus d'un trafic crypté, Fortigate réduit la complexité avec une visibilité automatisée sur les applications, les utilisateurs et le réseau, et fournit des mesures de sécurité pour adopter les meilleures pratiques.

En plus de FortiGate, Fortinet dispose d'une vaste gamme de produits pour fournir une protection complète à toutes les facettes du réseau [12].

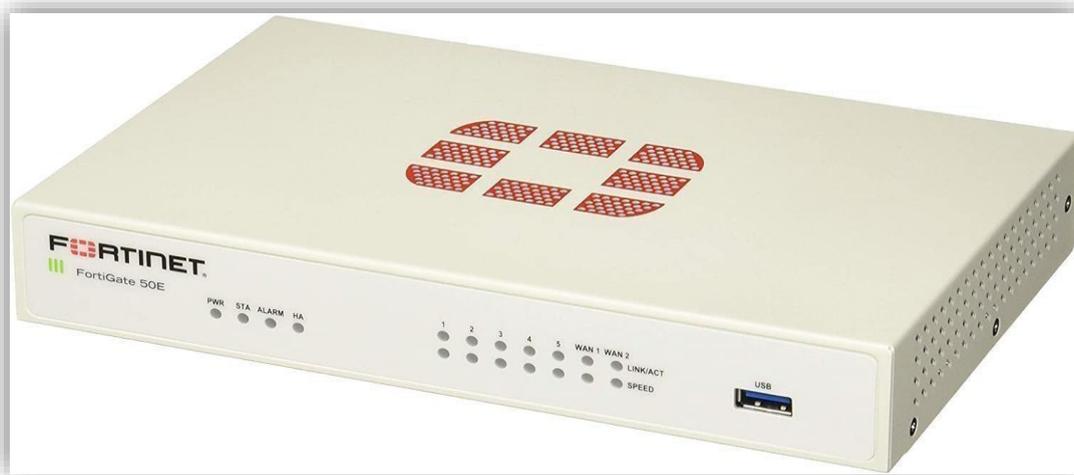


Figure 3.2 : Dispositif FortiGate

3.5. Les solutions de Fortigate (UTM) [12]

Il y a certaines caractéristiques qu'une solution UTM idéale doit posséder, tels que les services illustrés dans la figure 3.3.

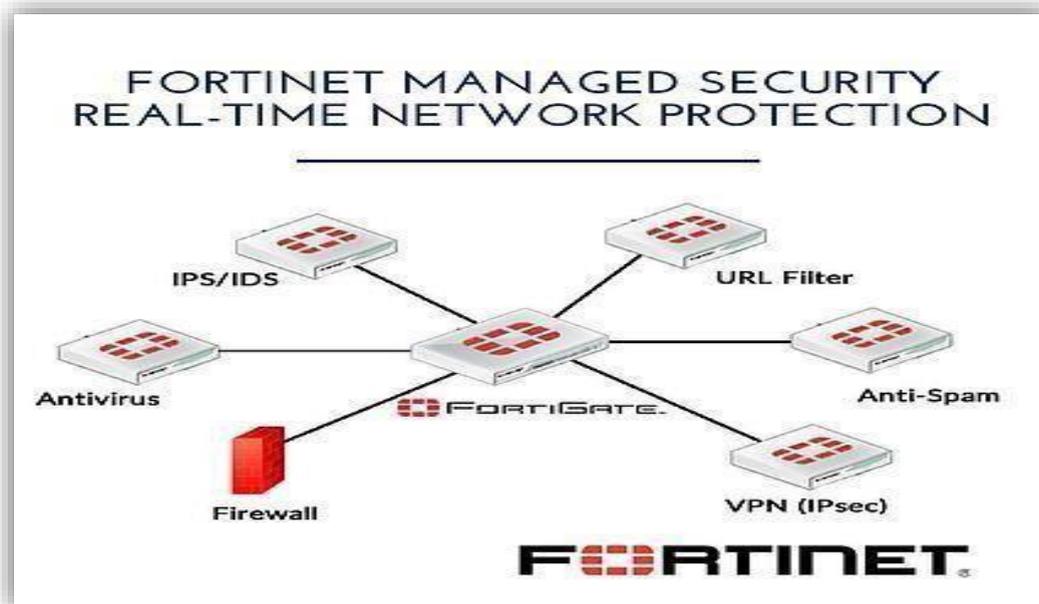


Figure 3.3 : Présentation des services FortiGate

a. Antivirus

Un UTM est livré avec un logiciel antivirus qui peut surveiller le réseau, puis détecter et empêcher les virus d'endommager le système ou ses appareils connectés. Cela se fait en tirant parti des informations contenues dans les bases de données de signatures, qui sont des entrepôts contenant les profils de virus, pour vérifier si certains sont actifs dans le système ou tentent d'y accéder.

Certaines des menaces que le logiciel antivirus d'un UTM peut arrêter incluent les fichiers infectés, les chevaux de Troie, les vers, les logiciels espions et autres logiciels malveillants.

b. Anti-malwares

La gestion unifiée des menaces protège le réseau contre les logiciels malveillants en les détectant et en y répondant. Un UTM peut être préconfiguré pour détecter les logiciels malveillants connus, les filtrer des flux de données et les empêcher de pénétrer dans le système. L'UTM peut également être configuré pour détecter les nouvelles menaces de logiciels malveillants à l'aide d'une analyse heuristique, qui implique des règles qui analysent le comportement et les caractéristiques des fichiers. Par exemple, si un programme est conçu pour empêcher le bon fonctionnement de la caméra d'un ordinateur, une approche heuristique peut signaler ce programme comme un logiciel malveillant.

Un UTM peut également utiliser le sandboxing comme mesure anti-malware. Avec le sandboxing, une cellule à l'intérieur de l'ordinateur est confinée à un bac à sable qui capture le fichier suspect. Même si le logiciel malveillant est autorisé à s'exécuter, le bac à sable l'empêche d'interagir avec d'autres programmes de l'ordinateur.

c. Pare-feu (firewalls)

Un pare-feu a la capacité d'analyser le trafic entrant et sortant à la recherche de virus, de logiciels malveillants, d'attaques de phishing, de spam, de tentatives d'intrusion sur le réseau et d'autres menaces de cybersécurité. Étant donné que les pare-feu UTM examinent à la fois les données entrantes et sortantes du réseau, ils peuvent également empêcher les appareils de ce dernier d'être utilisés pour propager des logiciels malveillants vers d'autres réseaux qui s'y connectent.

d. Prévention des intrusions (IPS)

Un système UTM peut fournir à une organisation une capacité de prévention des intrusions, qui détecte puis prévient les attaques. Cette fonctionnalité est souvent appelée système de détection d'intrusion (IDS) ou système de prévention d'intrusion (IPS).

Pour identifier les menaces, un IPS analyse les paquets de données, à la recherche de modèles connus qui existent dans les menaces lorsque l'un de ces motifs est reconnu, l'IPS arrête l'attaque. Dans certains cas, un IDS se contentera de détecter le paquet de données dangereux, et une équipe informatique pourra alors choisir comment elle souhaite traiter la menace.

Les mesures prises pour arrêter l'attaque peuvent être automatisées ou exécutées manuellement. L'UTM enregistrera également l'événement malveillant. Ces journaux peuvent ensuite être analysés et utilisés pour empêcher d'autres attaques à l'avenir.

e. VPN (Virtual Privat Networking)

Les fonctionnalités d'un réseau privé virtuel (VPN) fournies avec une Appliance UTM fonctionnent de la même manière qu'une infrastructure VPN classique. Un VPN crée un réseau privé qui passe par un réseau public, donnant aux utilisateurs la possibilité d'envoyer et de recevoir des données via le réseau public sans que d'autres voient leurs données.

Toutes les transmissions sont cryptées, donc même si quelqu'un devait intercepter les données, cela leur serait inutile.

f. Filtrage web

La fonction de filtrage web d'un UTM peut empêcher les utilisateurs de voir des sites web spécifiques ou des URL (Uniform Resource Locator). Cela se fait en empêchant les navigateurs des utilisateurs de charger les pages de ces sites sur leur appareil. Des filtres web peuvent être configurés pour cibler certains sites en fonction des objectifs de l'organisation. Par exemple, si on souhaite empêcher les employés d'être distraits par certains sites de médias sociaux, il est possible d'empêcher ces sites de se charger sur leurs appareils lorsqu'ils sont connectés au réseau de l'entreprise.

g. Prévention de la perte de données

La prévention de la perte de données obtenue avec une Appliance UTM permet de détecter les violations de données et les tentatives d'exfiltration, puis de les prévenir. Pour ce faire, le système de prévention de la perte de données surveille les données sensibles et, lorsqu'il identifie une tentative de vol par un acteur malveillant, bloque la tentative, protégeant ainsi les données.

3.6. Avantages de l'utilisation d'une solution unifiée de gestion des menaces (UTM)

Parmi les avantages d'utilisation d'UTM [12] :

- Flexibilité et adaptabilité
- Intégration et gestion centralisées
- Rentabilité
- Sensibilisation accrue aux menaces de sécurité réseau
- Solution de sécurité plus rapide pour les entreprises

3.7. La Zone démilitarisée (DMZ)**Définition**

Une DMZ (anglais :De-Militarized Zone), ou « zone démilitarisée » est une partie du réseau local dont l'objectif est d'être accessible depuis l'extérieur du réseaux local, avec ou sans authentification préalable. En effet, pour des raisons à la fois techniques et stratégiques, les réseaux IP locaux (LAN) sont (paradoxalement) devenus des zones inaccessibles depuis internet.

Une des raisons du problème réside dans le fait que la pénurie d'adresses IP nous a mène à utiliser, pour les machines du LAN, des adresses dites « privées ». Ces adresses ne doivent jamais être routées par la passerelle du LAN, et sont donc déconnectées d'internet. Evidemment, du point de vue de la sécurité, cela est un avantage ; cependant, la raison même de l'existence des réseaux est de faire communiquer les machines, pas de les isoler. Il faut alors soit acheter une adresse public supplémentaire, soit utiliser une astuce au niveau de la passerelle pour qu'au moins un des serveurs du LAN possède une identité sur Internet [8].

3.7.1. La sécurité dans une DMZ

Une zone démilitarisée (DMZ) est un sous-réseau se trouvant entre le réseau local et le réseau extérieur.

Propriétés : Les connexion à la DMZ sont autorisées de n'importe où. Les connexions à partir de la DMZ ne sont autorisées qu'à l'extérieur.

Intérêt : Rendre des machines accessibles à partir de l'extérieur (possibilité de mettre en place des serveurs (DNS, SMTP, etc.).

L'installation de la DMZ ne pose pas de problème de sécurité intrinsèque : en effet, toutes ses communications sont en grande partie gérées en amont. D'autre part, l'utilisation du NAT rend très difficile (souvent impossible) l'accès direct à la DMZ par un éventuel pirate [8].

3.7.2. Architecture DMZ

Lorsque certaines machines du réseau interne ont besoin d'être accessibles de l'extérieur (serveur web, un serveur de messagerie, un serveur FTP public, etc.), il est souvent nécessaire de créer une nouvelle interface vers un réseau à part, accessible aussi bien du réseau interne que de l'extérieur, sans pour autant risquer de compromettre la sécurité de l'entreprise. On parle ainsi de « zone démilitarisé » pour désigner cette zone isolée hébergeant des applications mises à disposition du public. La DMZ fait ainsi office de zone tampon entre le réseau à protéger et le réseau hostile [9].

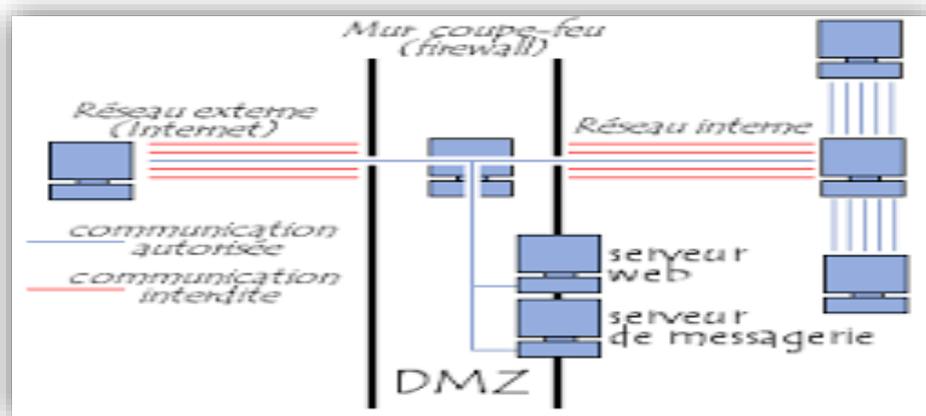


Figure 3.4 : schéma entre les réseaux à protéger

Les serveurs situés dans la DMZ sont appelés « bastions » en raison de leur position d'avant-poste dans le réseau de l'entreprise.

La politique de sécurité mise en œuvre sur la DMZ est généralement la suivante :

- Trafic du réseau externe vers la DMZ : **autorisé**.
- Trafic du réseau externe vers le réseau interne : **interdit**.
- Trafic du réseau interne vers la DMZ : **autorisé**.
- Trafic du réseau interne vers le réseau externe : **autorisé**.
- Trafic de la DMZ vers le réseau interne : **interdit**.
- Trafic de la DMZ vers le réseau externe : **refusé**.

La DMZ possède donc un niveau de sécurité intermédiaire, mais son niveau de sécurisation n'est pas suffisant pour y stocker des données critiques pour l'entreprise.

Il est à noter qu'il est possible de mettre en place des DMZ en interne afin de cloisonner le réseau interne selon différents niveaux de protection et ainsi éviter les intrusions venant de l'intérieur.

3.8. Conception

Pour la réalisation de notre travail, nous avons opté pour les outils suivant :

- Une machine virtuelle « VMware Workstation 15.1.0 »
- Un Fortigate (FortiVM)
- Une machine cliente Windows 7
- Windows Serveur 2016

3.8.1. Présentation de VMware Workstation

C'est la version station de travail du logiciel. Il permet la création d'une ou plusieurs machines virtuelles au sein d'un même système d'exploitation (généralement Windows ou linux), ceux-ci pouvant être reliés au réseau local avec une adresse IP différente, tout en étant sur la même machine physique (machine qui existe réellement). Il est possible de faire fonctionner plusieurs machines virtuelles en même temps, la limite correspondant aux performances de l'ordinateur hôte. La version linux présente l'avantage de pouvoir sauvegarder les fichiers de la machine virtuelle pendant son fonctionnement [4].

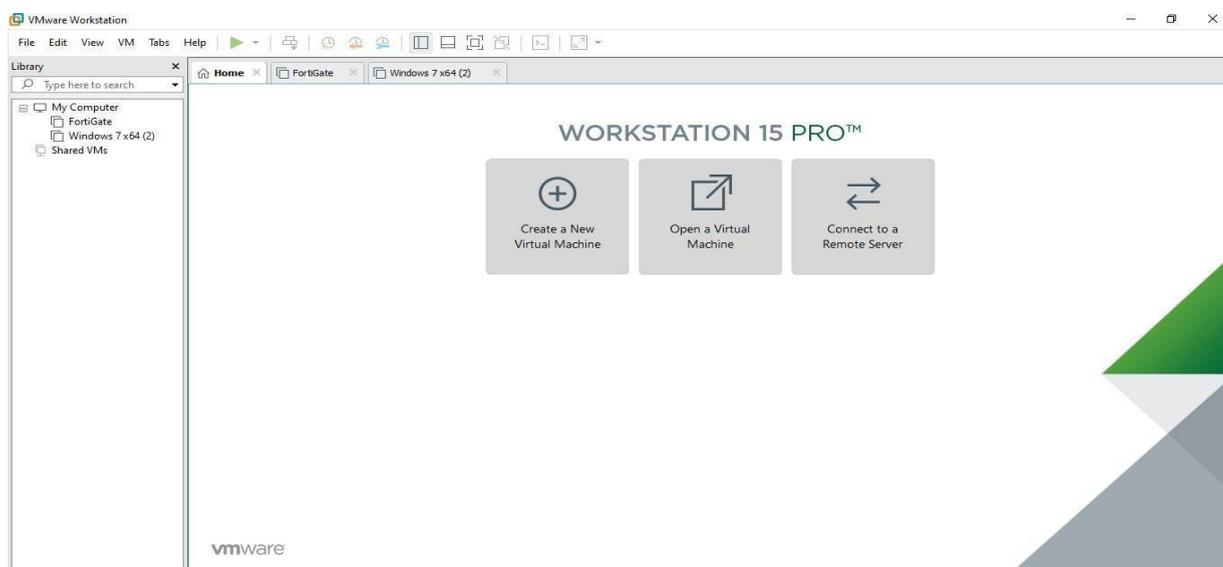


Figure 3.5 Interface d'accueil de VMware

3.8.2. Présentation de FortiGate-VM [13]

FortiGate-VM est un logiciel de pare feu (firewall) pour les professionnels, un pare-feu de nouvelle génération rapide et sécurisé.

Les Appliances virtuelles FortiGate permettent d'atténuer les angles morts en mettant en œuvre des contrôles de sécurité critiques dans l'infrastructure virtuelle. Ils permettent également de mettre en place rapidement une infrastructure de sécurité à tout moment et en tout lieu.

Points forts de FortiGate-VM

- Accessibilité.
- Intégration de la prévention des intrusions.
- Visibilité et contrôle des applications.
- Prise en charge des environnements physiques et virtuels.
- Identification et contrôle des menaces d'applications évasives.

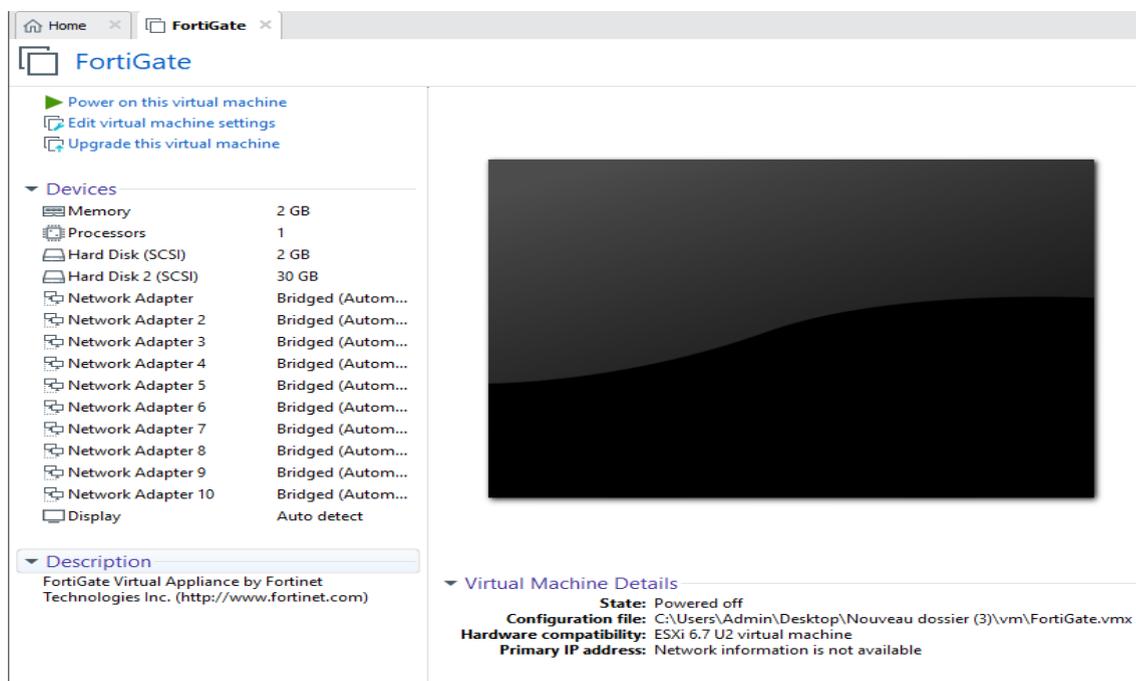


Figure 3.6: interface d'accueil de Fortigate

3.8.3. Présentation de Windows Server 2016

Windows server 2016 est un système d'exploitation pour serveur développé par Microsoft, il a été mis en disponibilité générale le 12 octobre 2016 et il a été développé en même temps que windows 10, basé sur l'architecture windows NT, il fournit toutes les capacités, fonctionnalités des mécanismes de fonctionnement d'un OS pour serveur standard.

Il propose ainsi différents services orientés serveur, comme la possibilité d'héberger un site web, la gestion des ressources entre les différents utilisateurs et applications, ainsi que des fonctionnalités de messagerie et de sécurité. Il est compatible avec la plupart des langages de programmation web et système de bases de données comme .NET CORE, PHP, MYSQL et MSSQL [14].

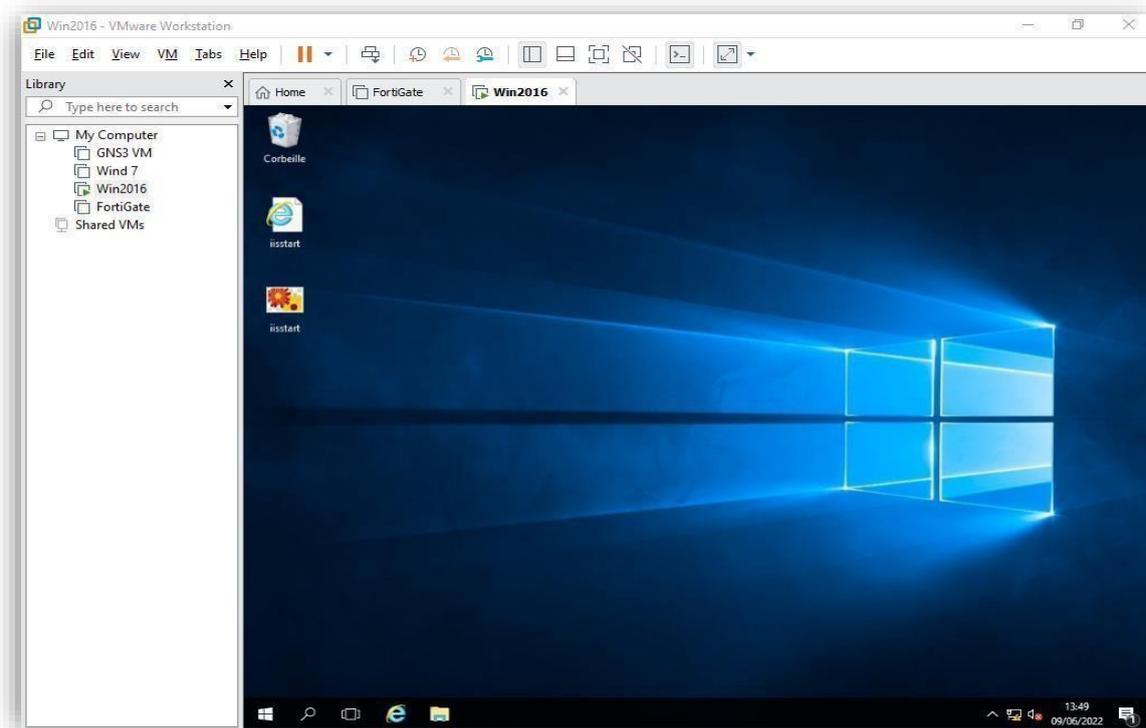


Figure 3.7 : Interface d'accueil de Windows serveur 2016

Conclusion

Dans ce chapitre, nous avons passé en revue les notions de base, le principe de fonctionnement ainsi que les principaux avantages des outils utilisés dans notre solution.

Le prochain chapitre sera porté sur le contexte du travail et l'implémentation de notre solution.

Introduction

L'implémentation est l'étape qui nous a permis de concrétiser les solutions et suggestions que nous avons proposées.

Dans ce chapitre, nous décrivons les outils utilisés, ainsi que les principales étapes de l'installation et configuration de Fortigate.

4.1. Prérequis

Pour la réalisation de notre travail, nous disposons des paramètres suivants :

- Une machine virtuelle « VMware-workstation15.1.0 »
- une machine cliente Windows 7, qui dispose d'une seule carte réseau
- un serveur 2016
- un FortiVM qui dispose de trois cartes réseaux, une pour l'interface WAN, la seconde pour l'interface LAN et la 3ème carte est dédiée à l'interface DMZ.

Voici la topologie que nous avons utilisée :

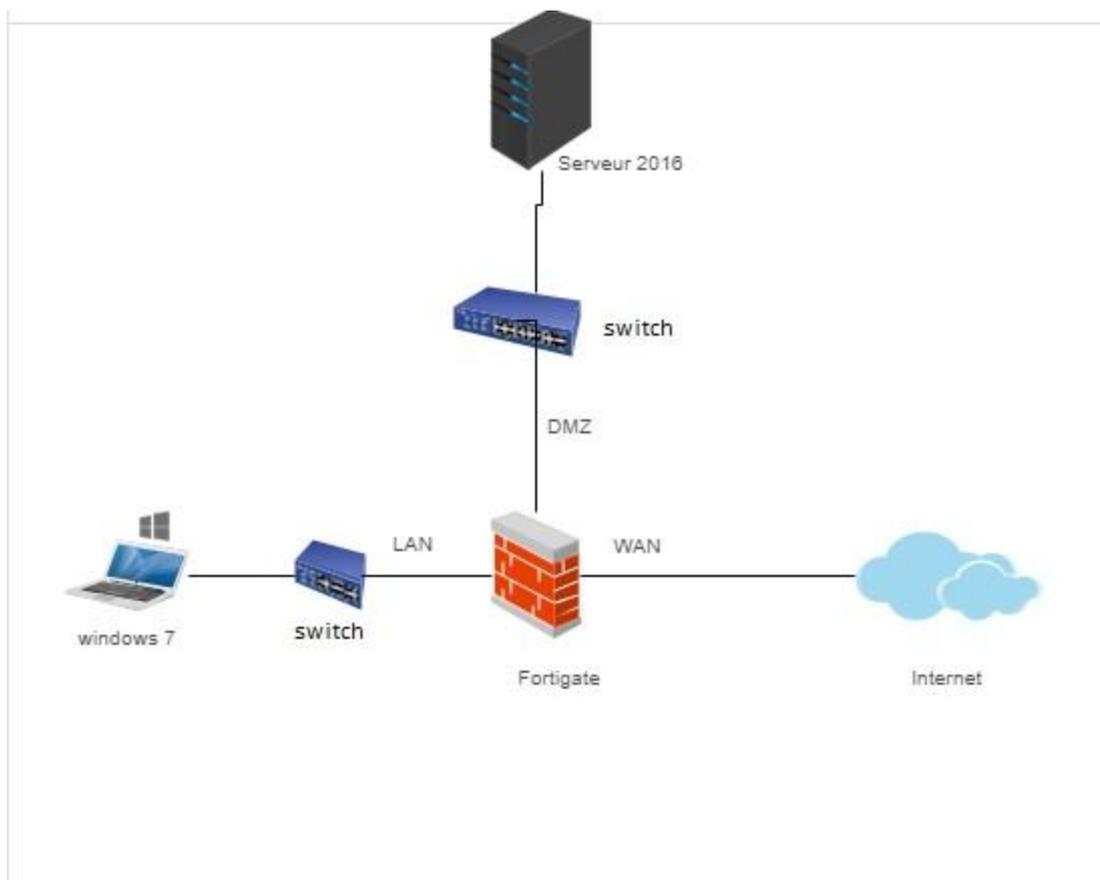


Figure 4.1 : Architecture réseau avec Fortigate

4.2. Installation de Fortigate

4.2.1. Téléchargement de Fortigat VM

Nous devons simplement aller sur le site de support de Fortinet« <https://support.fortinet.com> » et après connexion, nous pouvons télécharger l'image qui nous convient.

Nous téléchargeons ensuite le fichier ZIP qui contient des fichiers au format OVF, et à l'intérieur du dossier (après avoir extrait le ZIP) on trouve plusieurs fichiers correspondant à notre machine virtuelle.

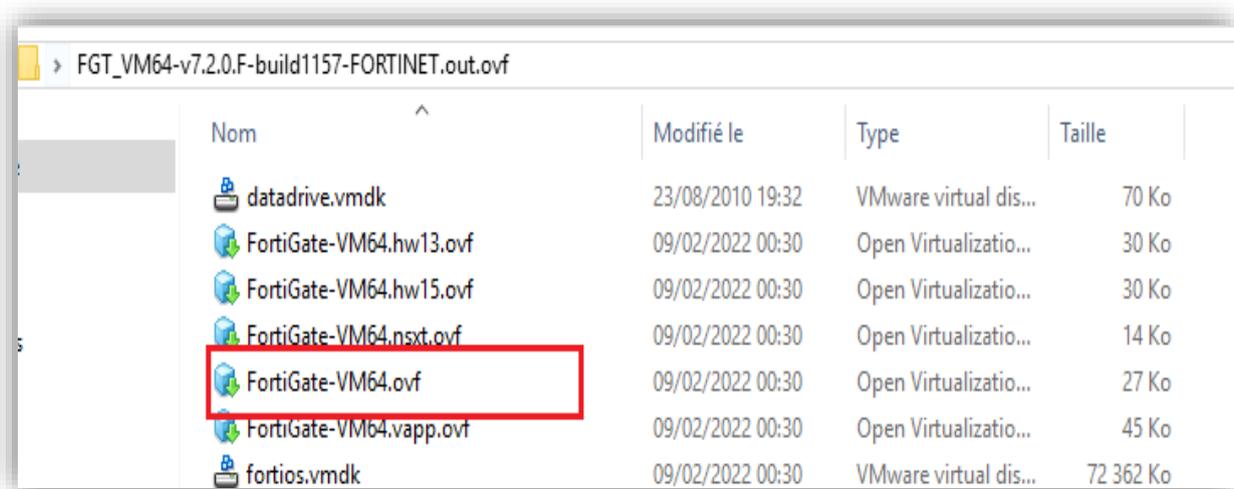


Figure 4.2 : Fichier de FortigateVm

Il existe plusieurs modèles que nous pouvons utiliser dans le programme VM, celui qui nous intéresse ici est vm64.ovf.

4.2.2. Installation de Fortigate sur VMWare Workstation

Après avoir téléchargé FortigatVM, nous passons à l'installation sur la vmware en cliquant sur l'onglet « open » dans la vmware et en choisissant l'image présentée dans la **Figure 4.2**.

Nous choisissons ensuite un nom pour la machine virtuelle, puis en cliquant sur « import », cela importera la machine virtuelle.

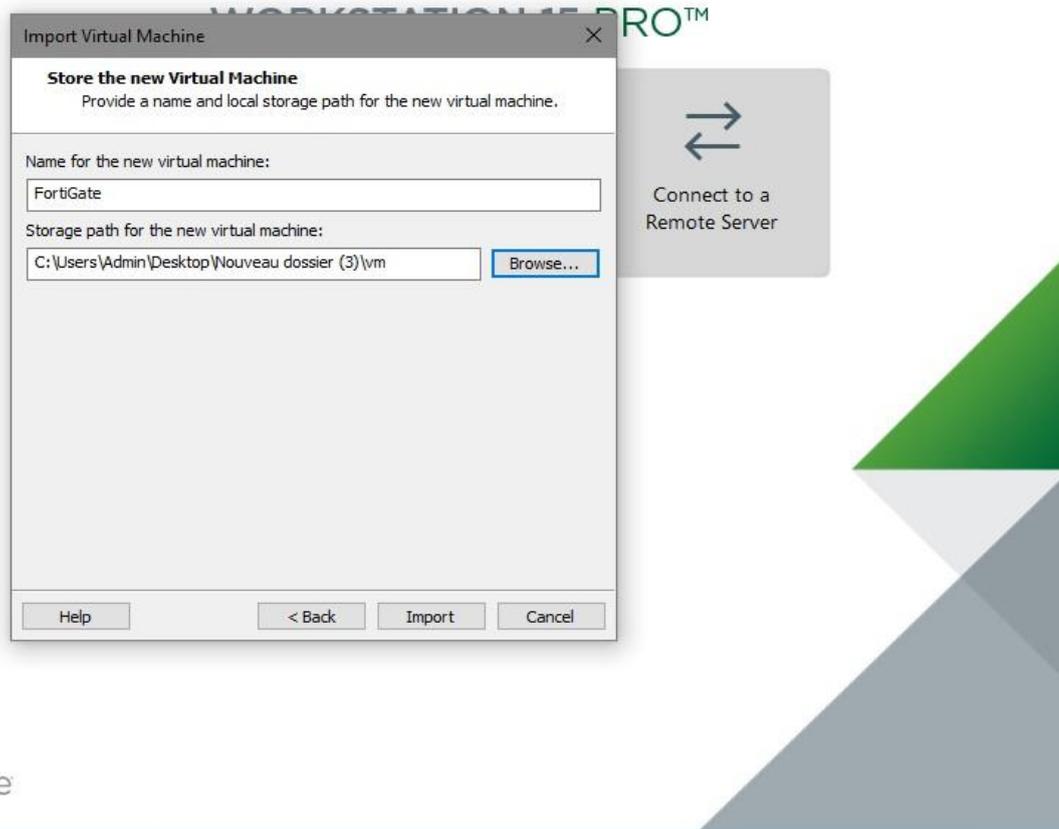


Figure 4.3 : Importation de l'image Fortigate sur la VMWare

Après quelques secondes, la VM FortiGate sera importée sur le poste de travail VMWare avec dix interfaces, nous pouvons modifier simplement les interfaces réseau virtuelles, la mémoire Et le processeur attribués. Dans notre cas, nous avons alloué 2 Go de RAM et 1 processeur. Afin de lancer notre machine, il suffit de cliquer sur « power on this virtual machine »

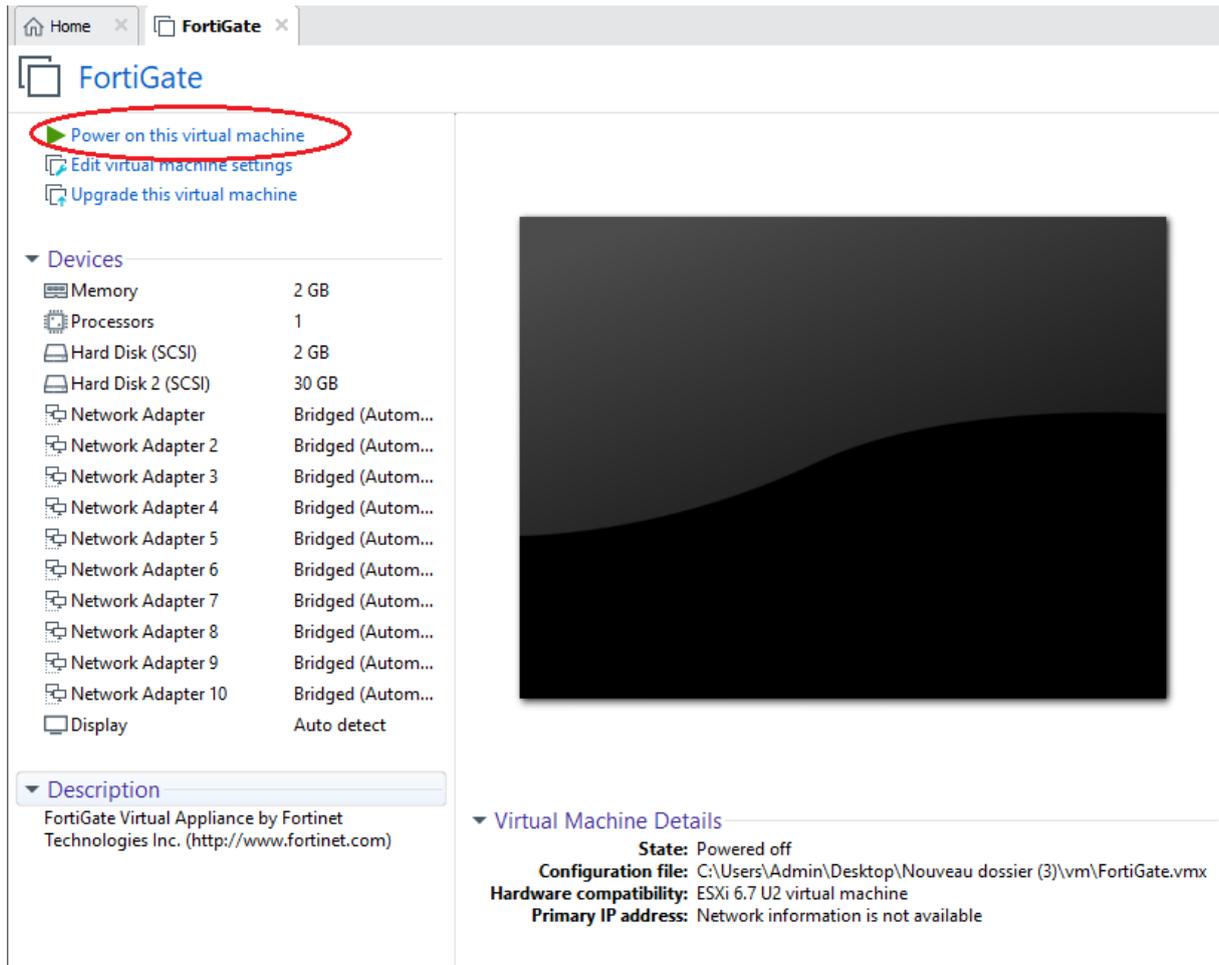


Figure 4.4 : Machine virtuelle de Fortigate.

Nous laissons le système démarrer de lui-même et après quelques secondes, nous arrivons à l'écran présenté dans la **figure 4.5**. Le nom d'utilisateur de la VM sera « admin » avec un mot de passe.

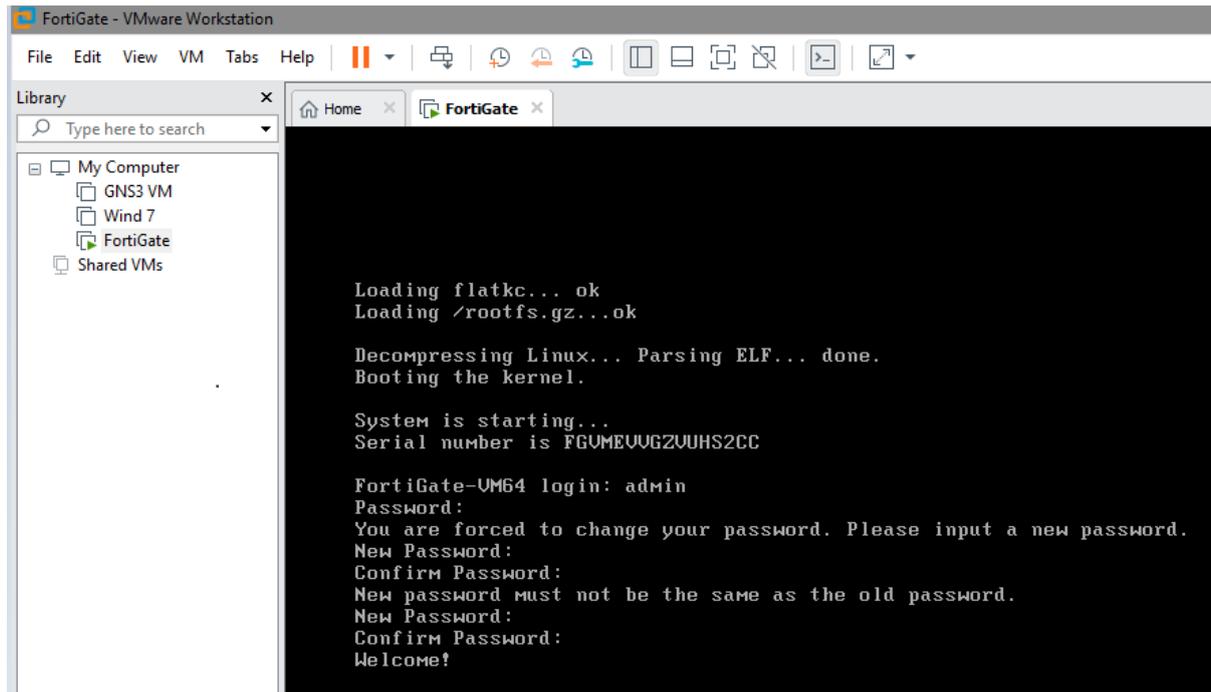


Figure 4.5 : Ecran de configuration de Fortigate

4.3. Configuration des interfaces de Fortigate

Comme nous l'avons vu dans la **Figure 4.1**, nous n'avons pas besoin de l'ensemble des 10 interfaces, à la place, nous utiliserons trois interfaces. La première (Port2) pour le LAN, la seconde (Port1) pour le WAN, et la troisième (Port3) pour la DMZ.

4.3.1. Configuration de l'interface LAN

Nous cliquons d'abord sur le bouton Démarrer de Windows > Virtual Network Editor, nous utilisons donc l'adaptateur VMnet2 comme « host-only ». Après cela, nous devons fournir une adresse IP statique (mode DHCP désactivé). Dans notre cas nous avons utilisé l'adresse 192.168.11.0/24 pour le vmnet2.

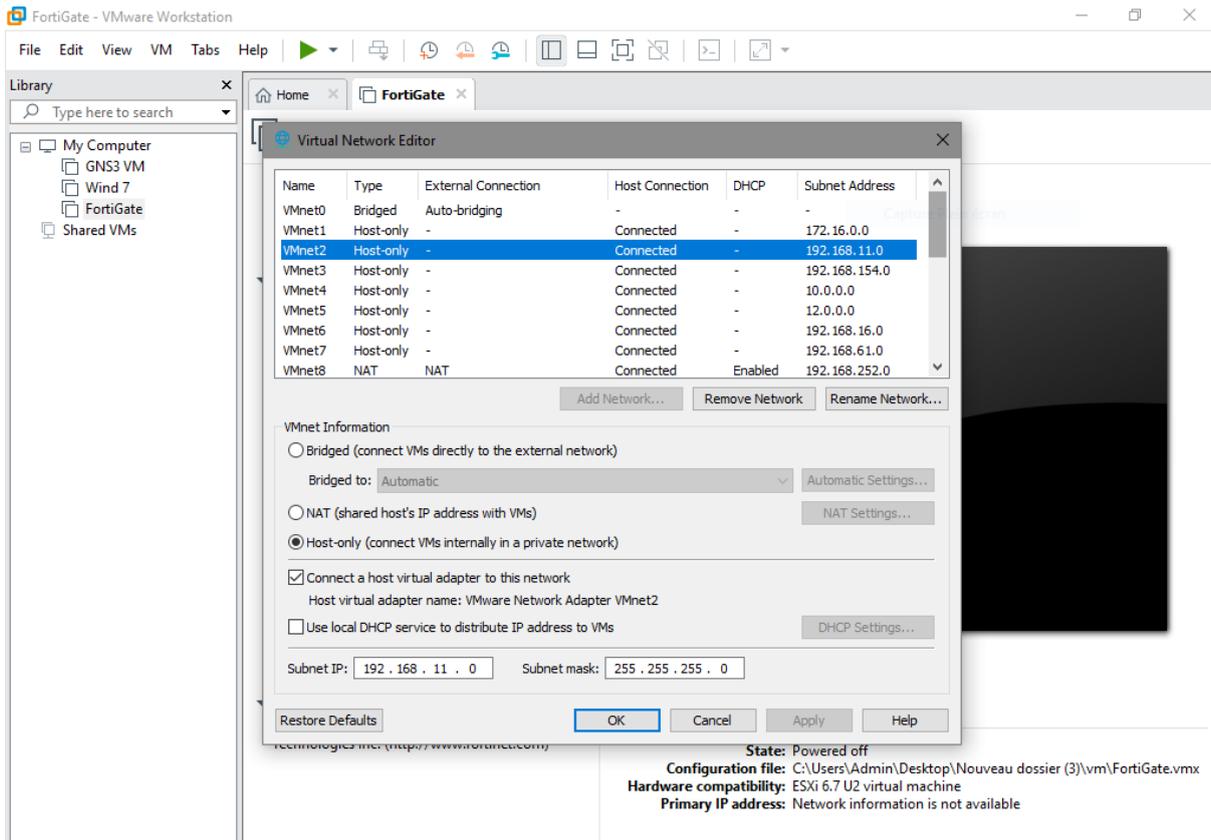


Figure 4.6 : Configuration de l'interface LAN coté vmware

Nous attribuons ensuite le Switch virtuel (Vmnet2) au port2 (LAN).

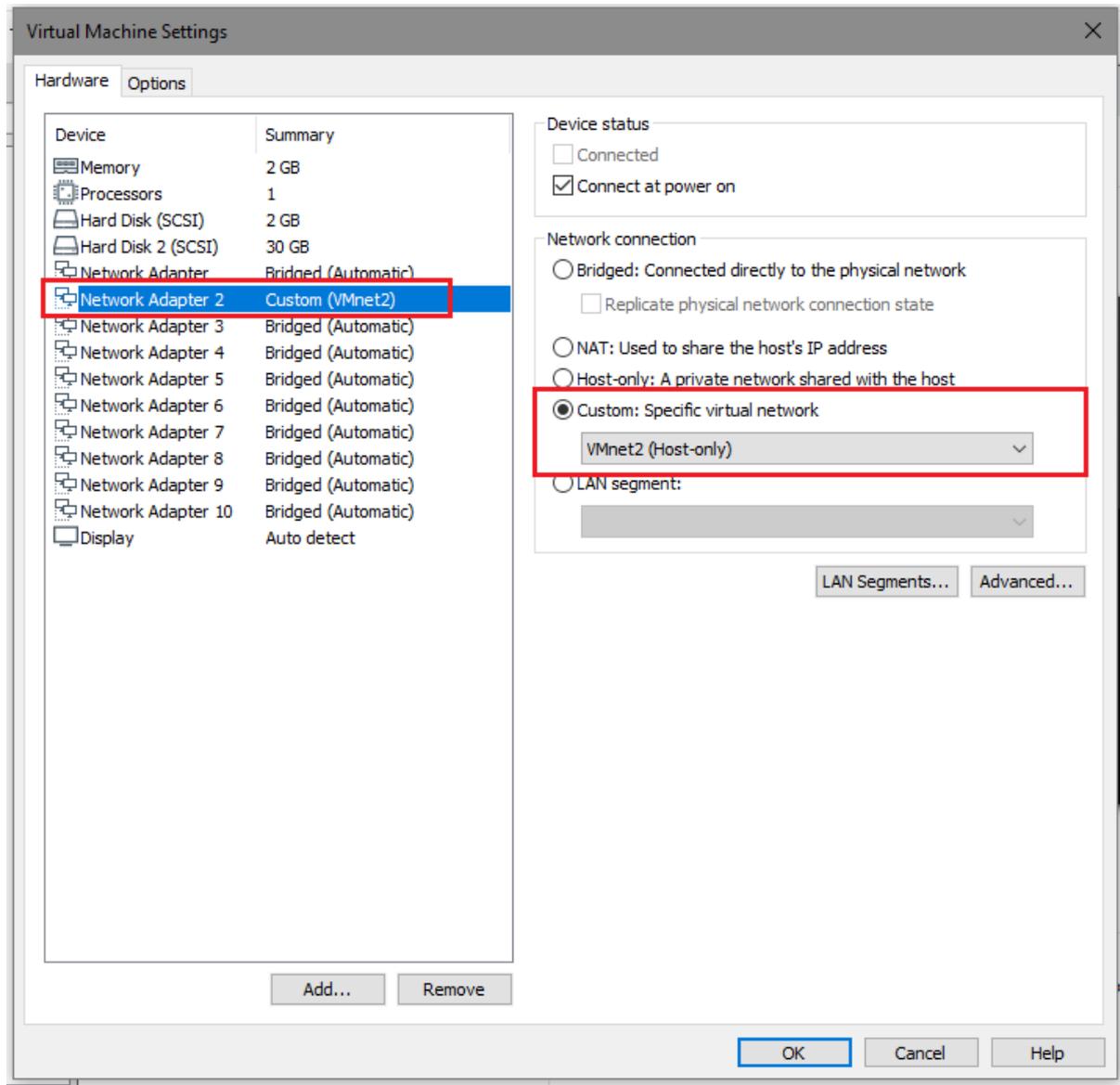


Figure 4.7 : Attribution du Switch virtuel au port 2

Nous configurons maintenant une adresse IP pour le port 2. La deuxième interface virtuelle sera l'interface LAN. Alors, nous devons attribuer une adresse IP sur la même plage que celle que nous avons attribuée dans la **Figure 4.6**. Pour ce faire, nous exécutons les commandes suivantes.

```
FortiGate-UM64 # config system interface
FortiGate-UM64 (interface) # edit port2
FortiGate-UM64 (port2) # set ip 192.168.11.254 255.255.255.0
FortiGate-UM64 (port2) # set mode static
FortiGate-UM64 (port2) # set allowaccess https http ping
FortiGate-UM64 (port2) # end_
```

Figure 4.8 : Ecran de configuration de l'interface LAN

Maintenant, nous attribuons une adresse à notre machine physique.

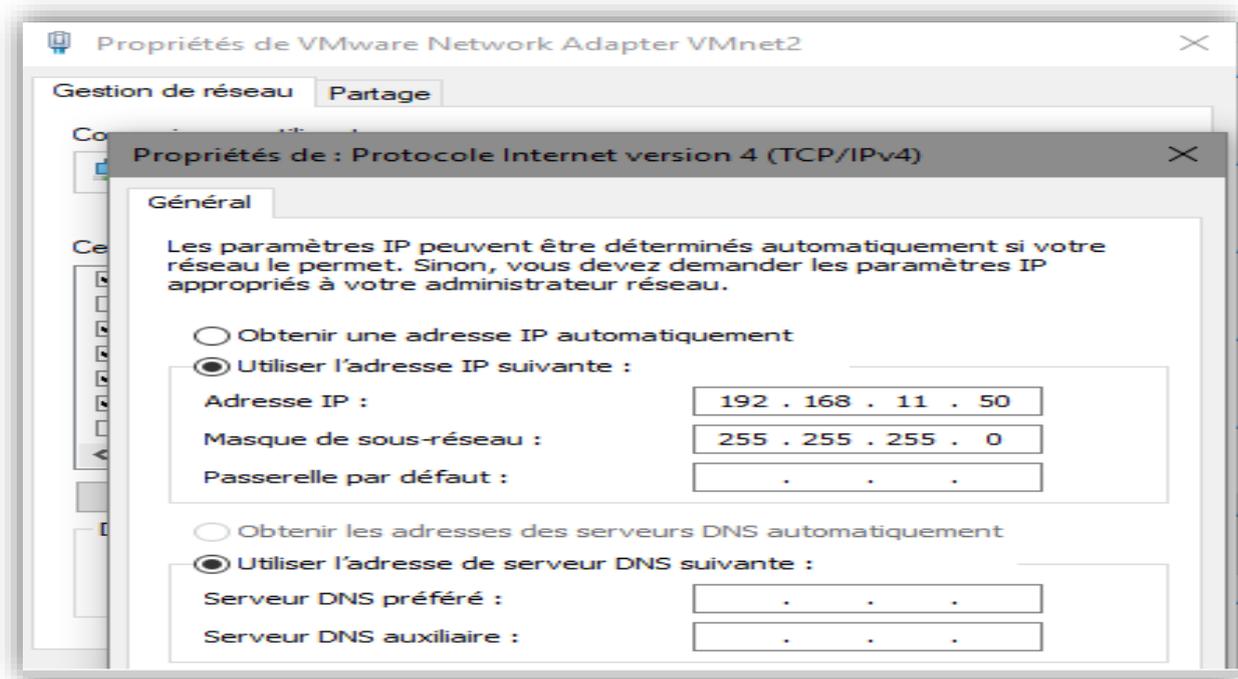


Figure 4.9 : Adresse de la machine physique

➤ Tester la connectivité

- Machine physique ➔ Fortigate

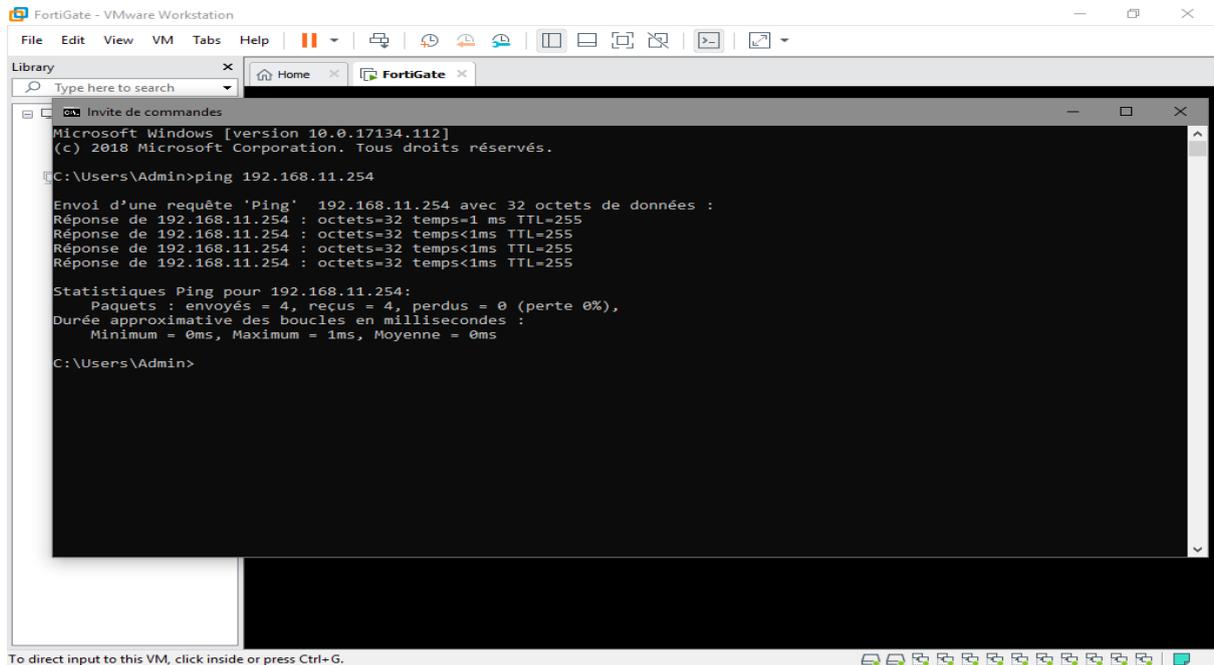


Figure 4.10 : Ping de la machine physique vers Fortigate

- Fortigate ➔ la machine physique

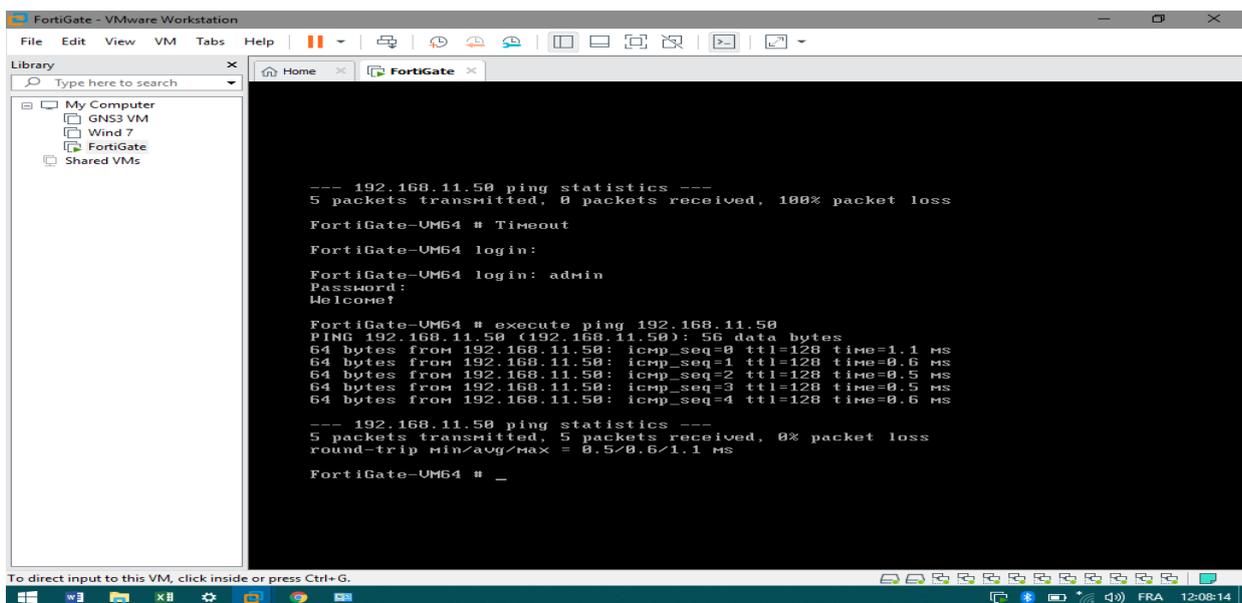


Figure 4.11 : Ping de Fortigate vers la machine physique

➤ **Accéder à l'interface graphique FortiGate**

Nous avons déjà l'adresse IP sur l'interface2. Nous continuons et accédons à l'interface graphique Web à l'aide de l'interface de gestion sur le port2. Qui est 192.168.11.254. Il faut donc taper <http://192.168.11.254> dans un navigateur web.

Nous pouvons nous connecter à la VM en utilisant le nom d'utilisateur « admin » et le mot de passe que nous avons défini à l'aide de la CLI.

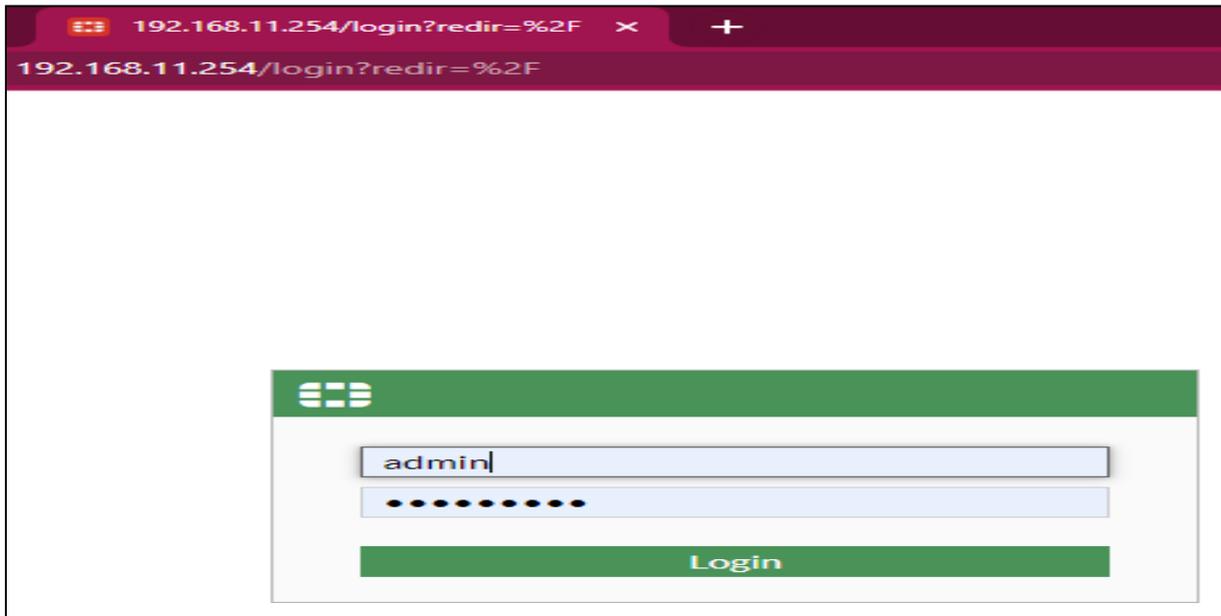


Figure 4.12 : Page d'identification de Fortigate

Maintenant, nous devons accéder à l'interface graphique de FortiGate.

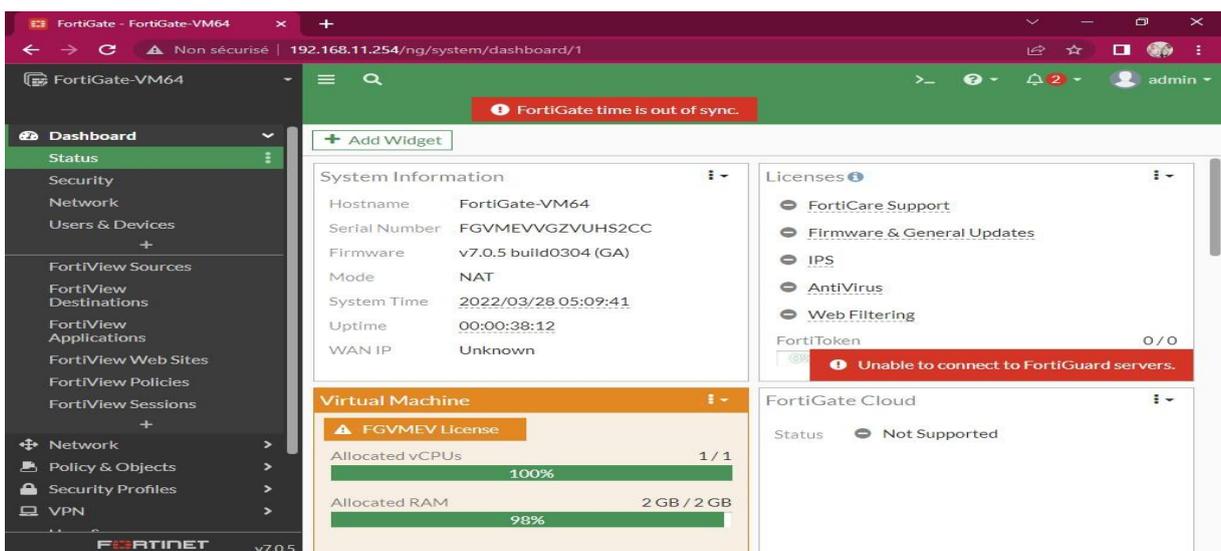


Figure 4.13 : Iinterface graphique du fortigate

4.3.2. Configuration de l'interface WAN

Pour la deuxième interface, nous allons utiliser le mode bridged (pont). De cette façon, une adresse automatique sera attribuée à l'interface WAN.

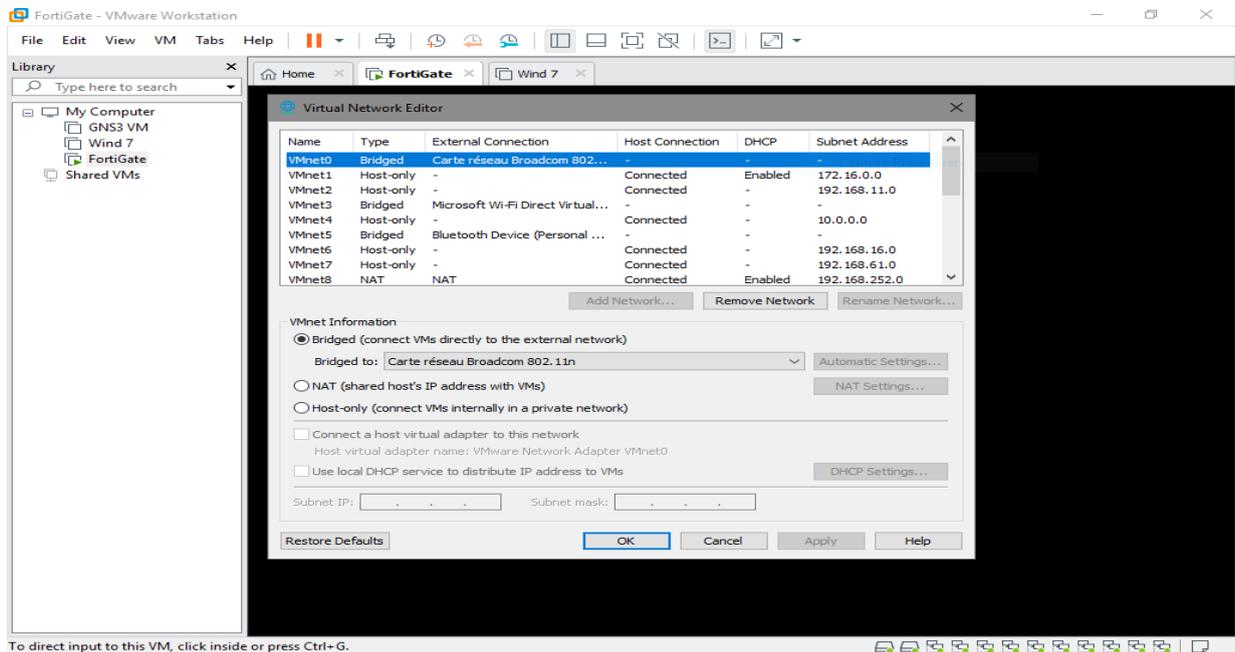


Figure 4.14 : Configuration de l'interface web au bridged

Nous attribuons ensuite le Switch virtuel (Vmnet0) au port1 (WAN).

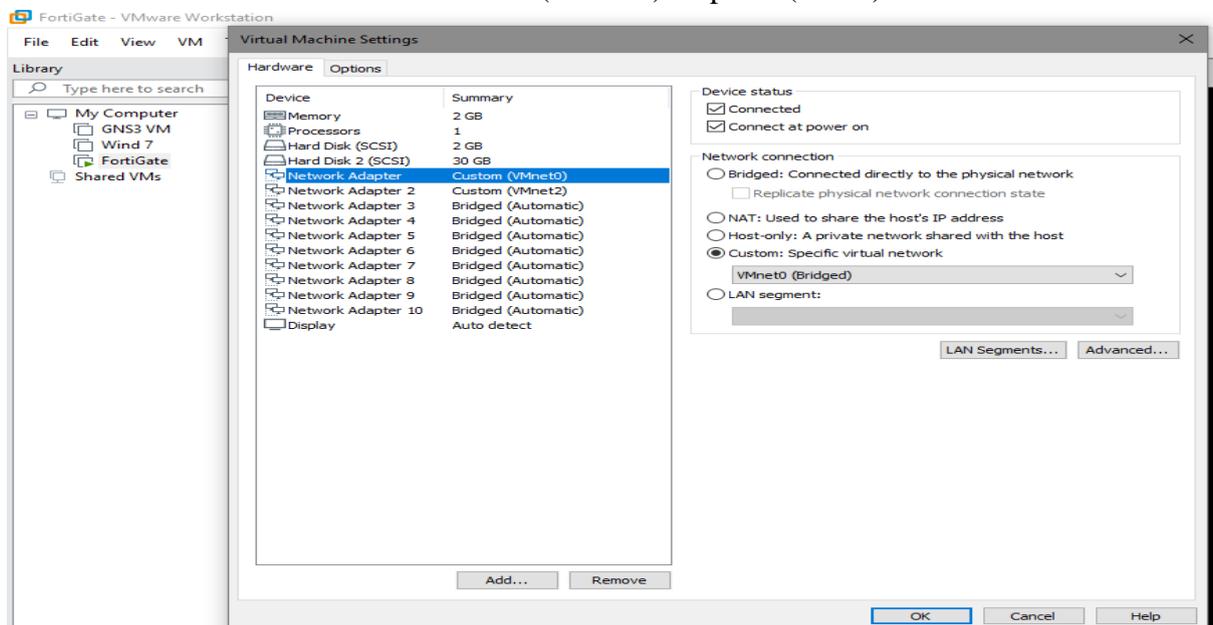


Figure 4.15 : Attribution d'un Switch virtuel au port 1

➤ Vérifier si le réseau a alloué une adresse IP à notre machine physique

Pour ce faire, il faut être connecté à internet (vérifier si nous avons eu l'adresse IP du DHCP de la BMT)

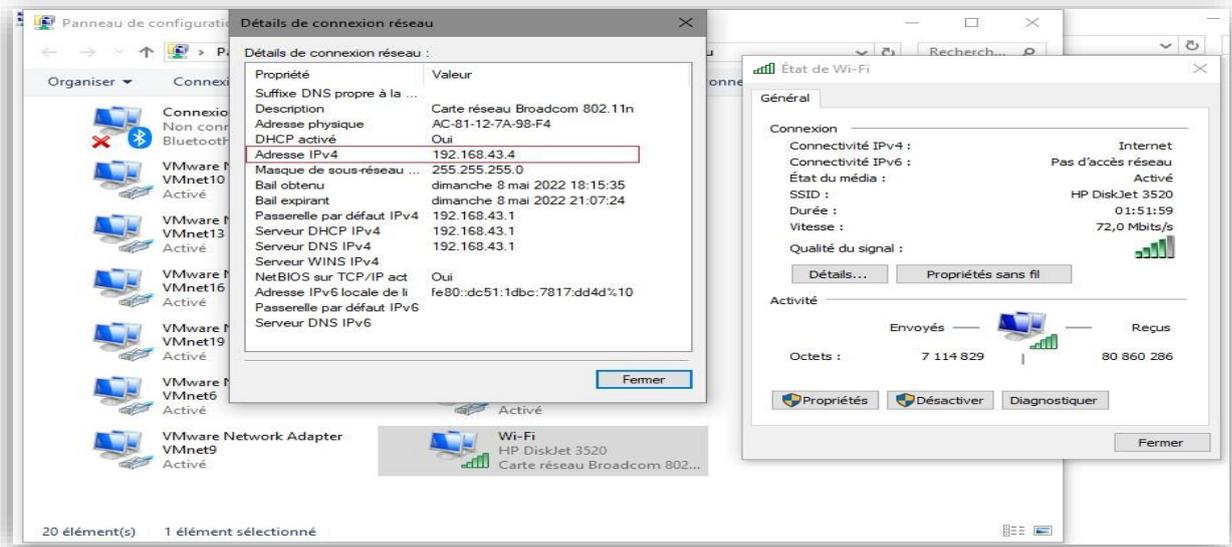


Figure 4.16 : Ecran de configuration de la carte réseau Ethernet

➤ Récupérer l'adresse IP du port WAN

Nous réglons le mode adressage sur DHCP pour permettre à l'équipement d'attribuer une adresse IP.

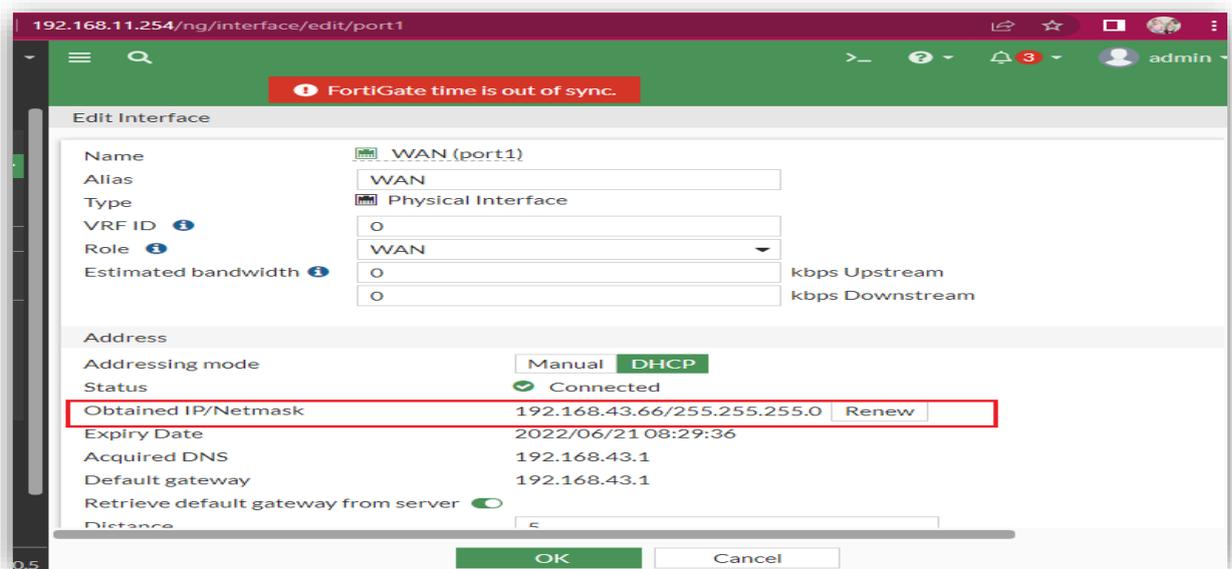


Figure 4.17 : Configuration de l'interface WAN (DHCP)

Nous avons déjà une machine Windows 7 fonctionnant sur FortiGate, mais nous devons la connecter au réseau de segments LAN (VMnet2) que nous avons créé.

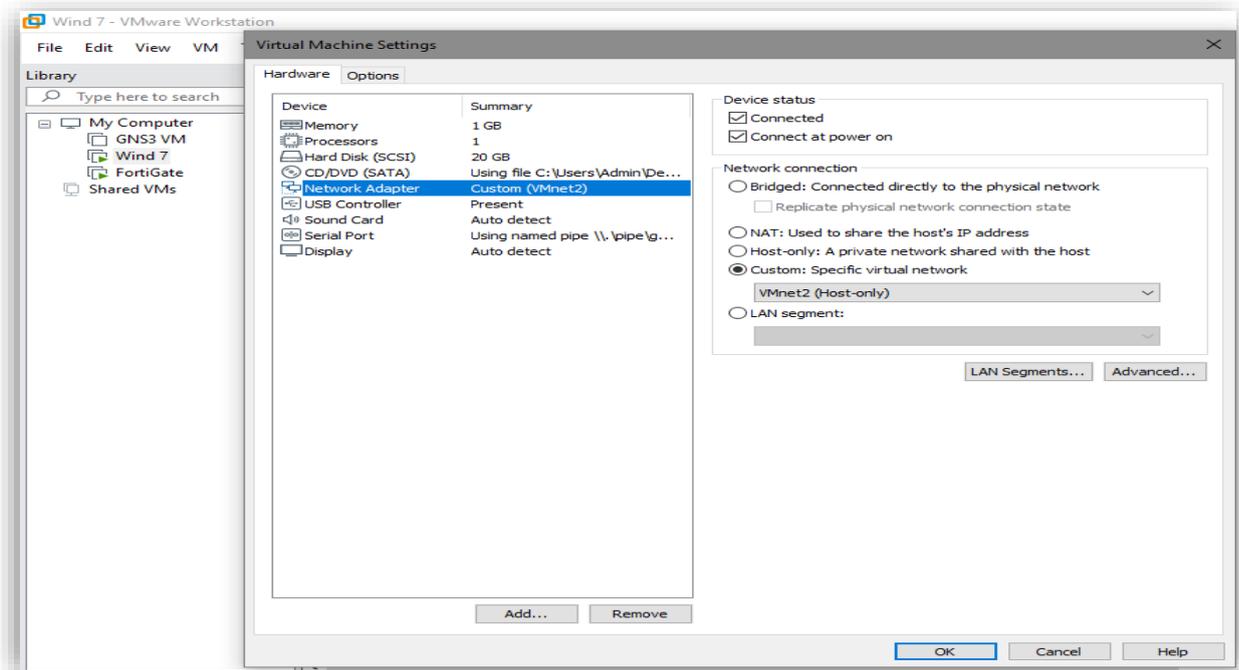


Figure 4.18 : Attribution switch 2 a l'interface

Nous donnons une adresse à notre client (windows 7) ainsi que l'adresse de la passerelle.

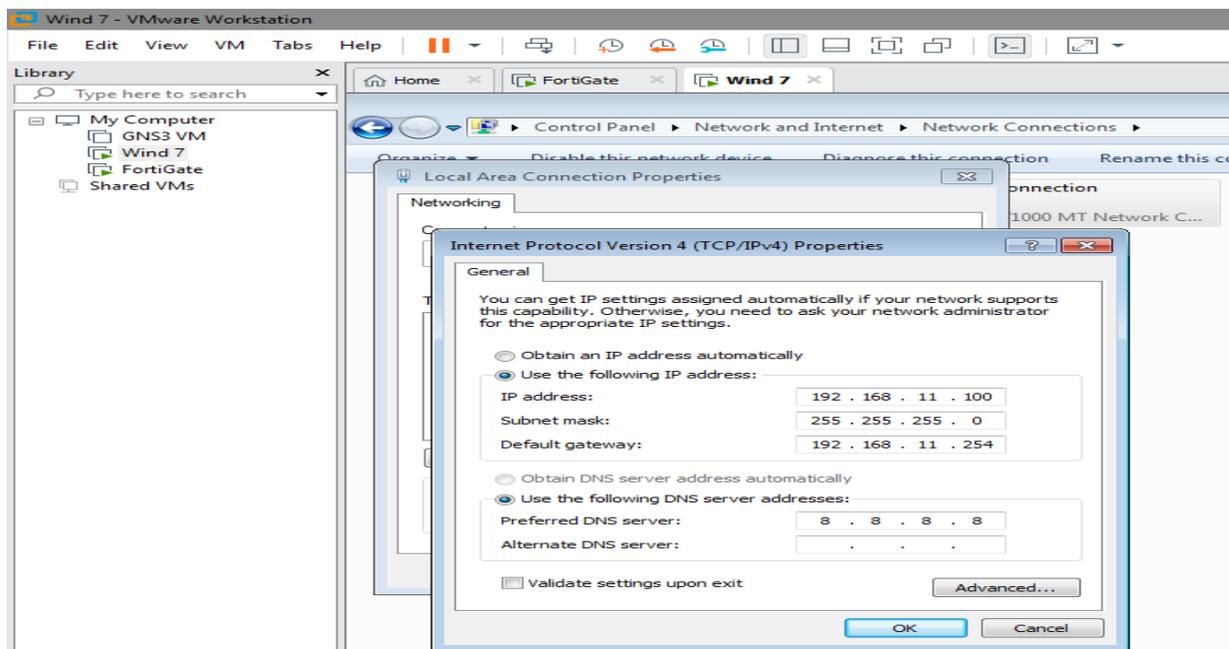


Figure 4.19 : Ecran de configuration de la carte réseau du client

- Tester la connectivité (ping)
 - Fortigate → client

```

FortiGate-UM64 # execute ping 192.168.11.100
PING 192.168.11.100 (192.168.11.100): 56 data bytes
64 bytes from 192.168.11.100: icmp_seq=0 ttl=128 time=1.4 ms
64 bytes from 192.168.11.100: icmp_seq=1 ttl=128 time=1.1 ms
64 bytes from 192.168.11.100: icmp_seq=2 ttl=128 time=1.1 ms
64 bytes from 192.168.11.100: icmp_seq=3 ttl=128 time=1.0 ms
64 bytes from 192.168.11.100: icmp_seq=4 ttl=128 time=0.9 ms

--- 192.168.11.100 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.9/1.1/1.4 ms

FortiGate-UM64 #
    
```

Figure 4.20 : Ping de Fortigate vers le client

- Client → Fortigate

```

C:\Users\ne>ping 192.168.11.254

Pinging 192.168.11.254 with 32 bytes of data:
Reply from 192.168.11.254: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.11.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\ne>_
    
```

Figure 4.21 : Ping de la machine client vers Fortigate

➤ Configuration des adresses objets

Avant de continuer et de créer une politique, nous créons un objet Adresse, que l'on peut appeler ultérieurement dans la création de la politique. Nous nous rendons dans :

Policy&Objects ->Addresses -> Create New-> Address.

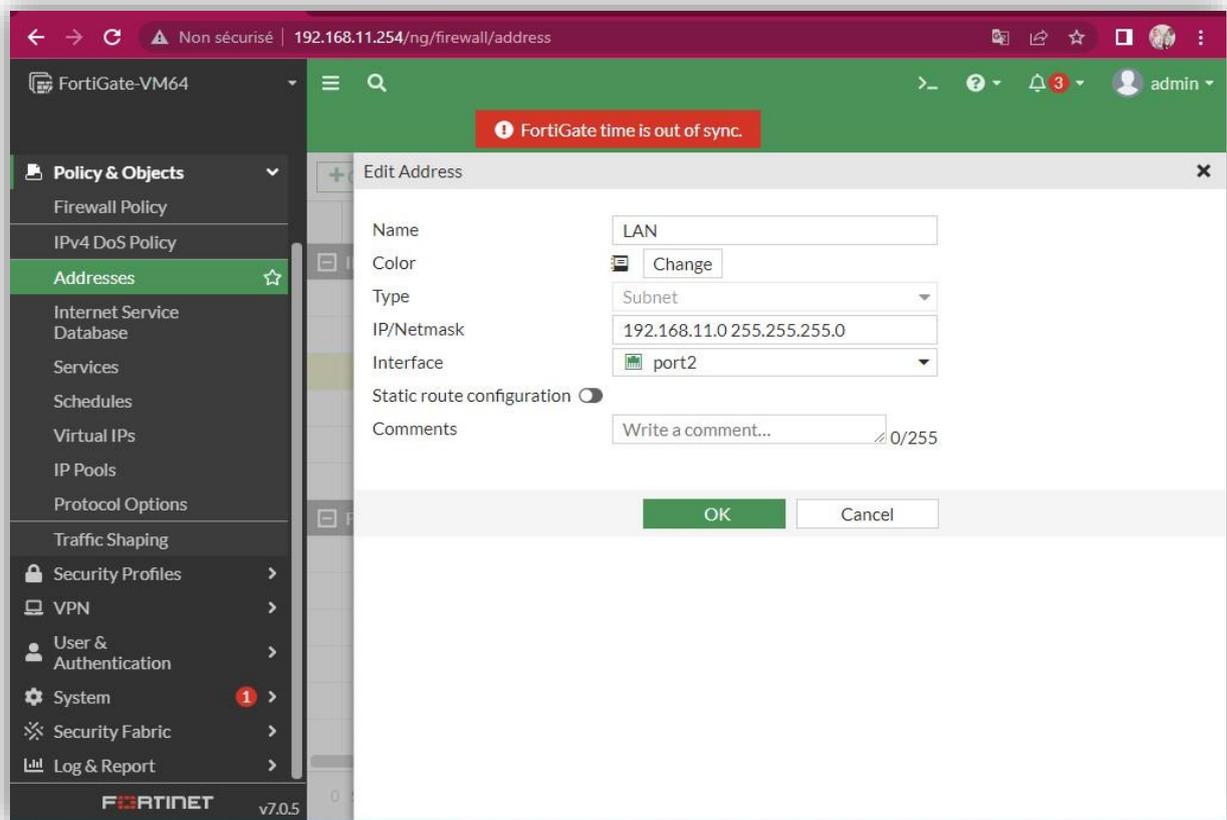


Figure 4.22 : Création de l'adresse objet

➤ Création d'une politique

Nous allons désormais créer une politique de sécurité et de NAT afin que les VM du côté LAN aillent sur Internet.

Nous nous rendons dans: **Policy&Objects-> Firewall Policy-> Create Policy**

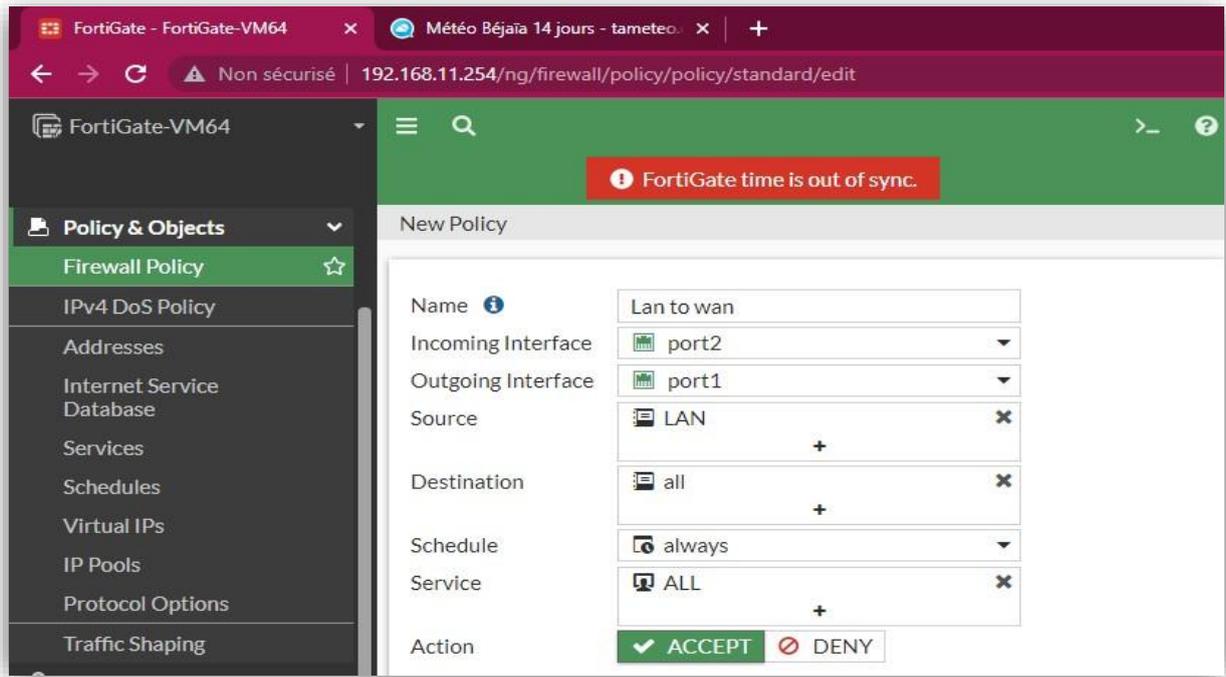


Figure 4.23 : Création de la politique LAN vers WAN

Nous devons nous assurer que l'action est définie sur ACCEPTER.

➤ **Configuration du NAT**

Un des avantages de FortiGate est que nous pouvons définir la politique NAT directement dans la politique de sécurité. Nous activons NAT et sélectionnons **Use Outgoing Interface Address**.

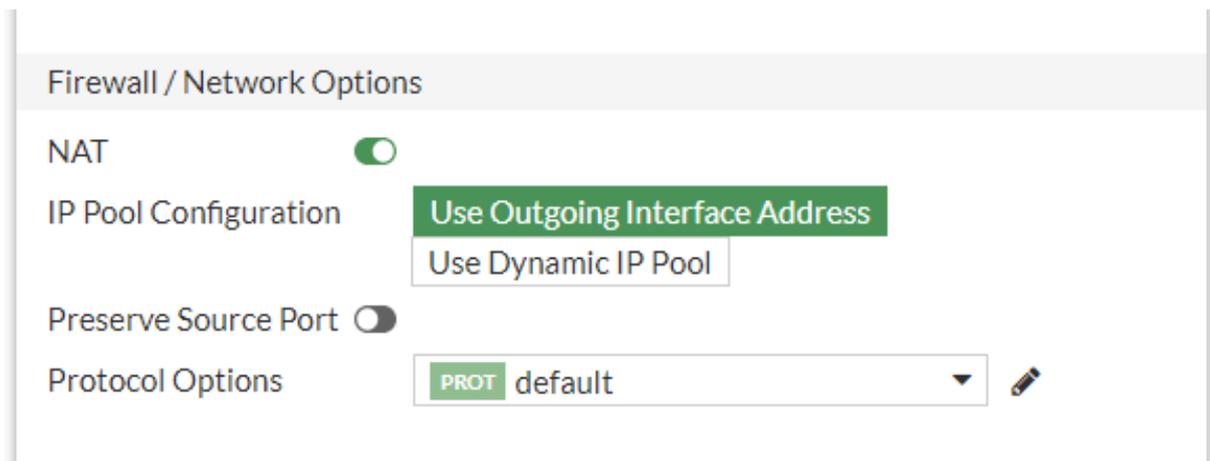


Figure 4.24 : Activation du NAT

Nous sélectionnons « Toutes les sessions » puis nous cliquons sur OK.

Name	Source	Destination	Schedule	Service	Action	NAT	Security
port2 → WAN (port1) 1							
LAN TO WAN	LAN	all	always	ALL	ACCEPT	Enabled	<div style="display: flex; gap: 5px;"> WEB facebook SSL certifi </div>

Figure 4.25 : Stratégie du LAN TO WAN

➤ Résultats

Si nous avons tout fait dans l'ordre, nous pourrons alors nous connecter automatiquement à Internet, à l'aide du PC sur le réseau interne.

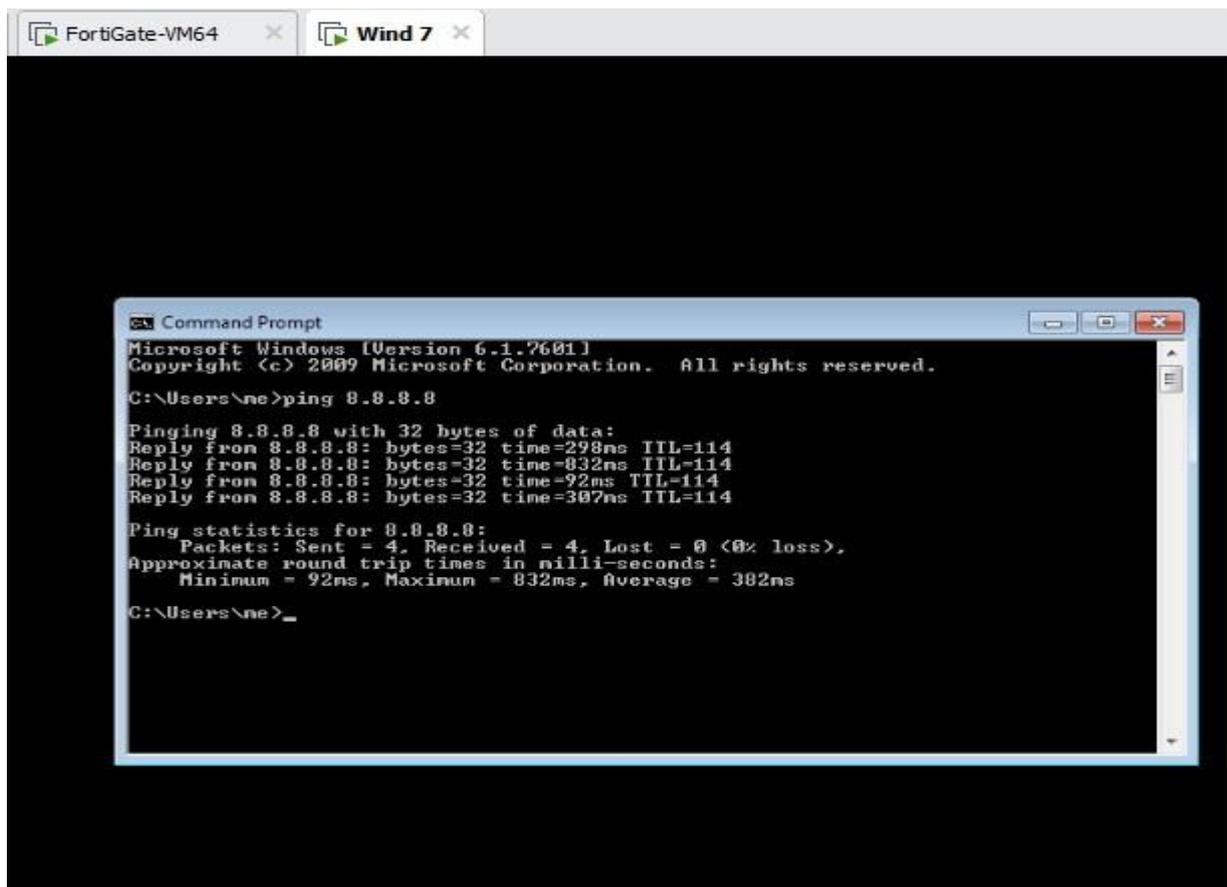


Figure 4.26 : Tester le ping vers google

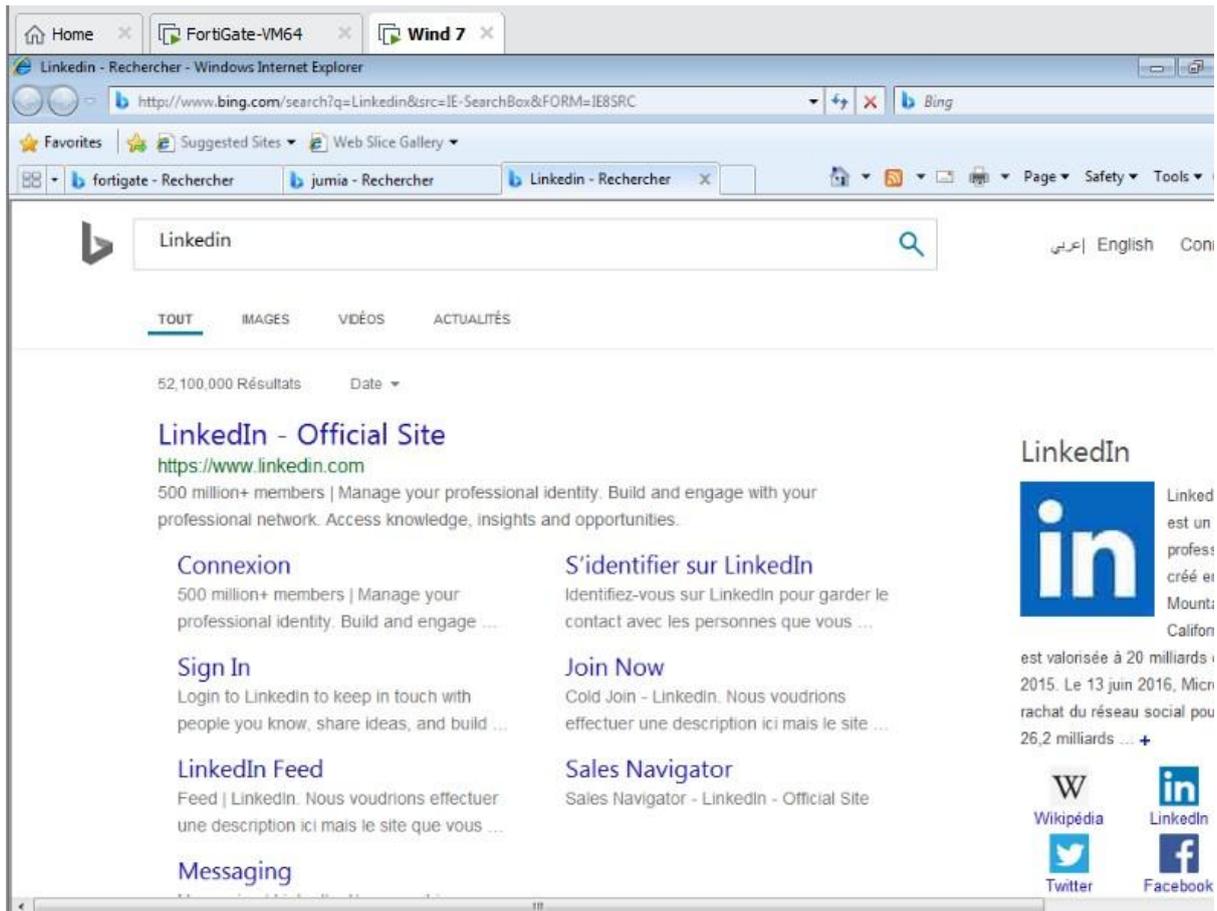


Figure 4.27 : Accéder au site internet (LinkedIn)

➤ Application des profils de sécurité

Cette section décrit comment ajouter des profils de protection aux règles.

Pour ajouter un profil de protection, il faut se rendre dans **fortigate > security profiles > web Filter>**

➤ **Création d'un filtre d'URL**

Pour créer un filtre d'URL dans l'interface graphique : nous cliquons sur **URL Filter**

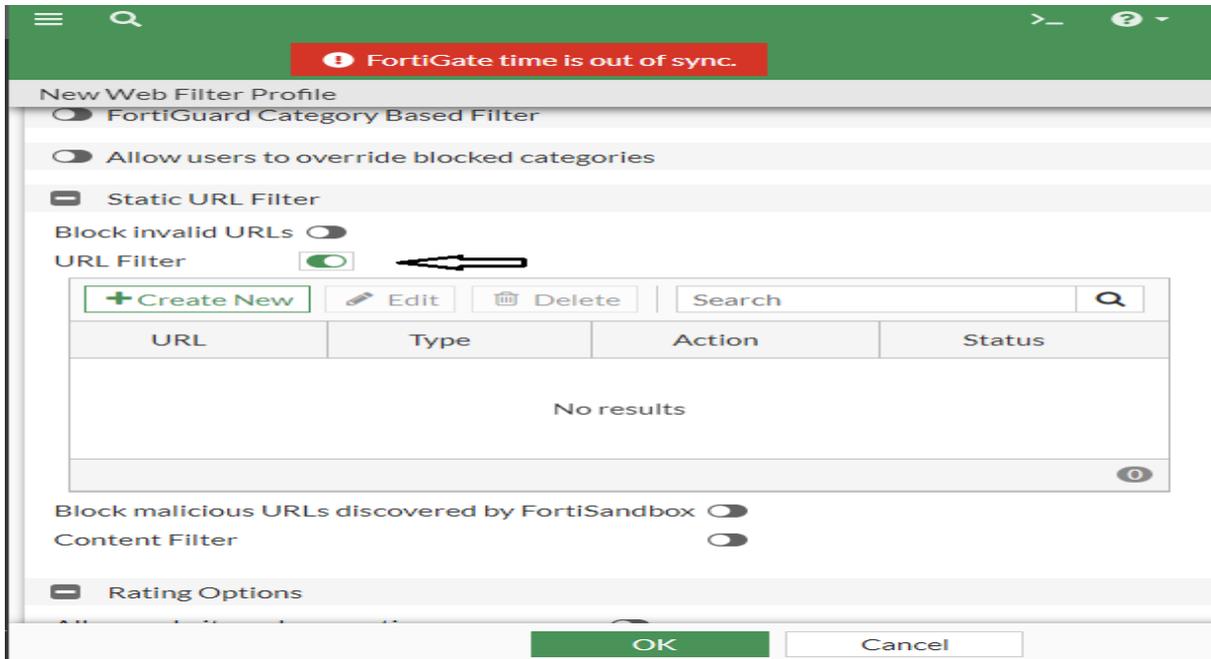


Figure 4.28 : Créer un nouveau web Filter

Sous Filtre d'URL, nous sélectionnons **create new** pour afficher le volet Nouveau filtre d'URL

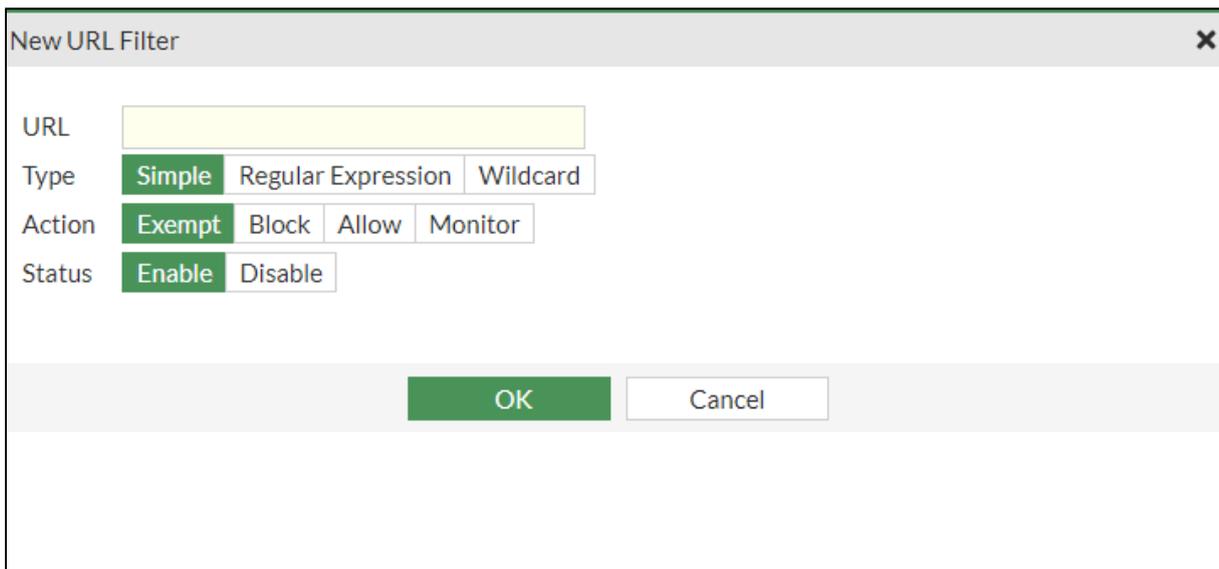


Figure 4.29 : Créer un nouveau URL Filter

➤ **Description du type de filtre d'URL**

- **Simple** : FortiGate essaie de correspondre strictement au contexte complet.
- **Regular Expression ou Wildcard**: FortiGate essaie de faire correspondre le modèle en fonction des règles des expressions régulières ou des caractères génériques.

➤ **Description de l'action de filtrage d'URL**

- **Exempt** : Le trafic est autorisé à contourner les filtres Web FortiGuard restants, webfilters, web script filters, antivirus scanning, et DLP proxy operations
- **Block** : Refuse ou bloque les tentatives d'accès à toute URL correspondant au modèle d'URL.
- **Allow** : Le trafic est transmis aux autres filtres Web FortiGuard, webfilters, web script filters, antivirus proxy operations, et DLP proxy operations.. Si l'URL n'apparaît pas dans la liste des URL, le trafic est autorisé.
- **Monitor** : Le trafic est traité de la même manière que allow action Pour l'action Monitor, un message de journal est généré chaque fois qu'un modèle de trafic correspondant est établi.

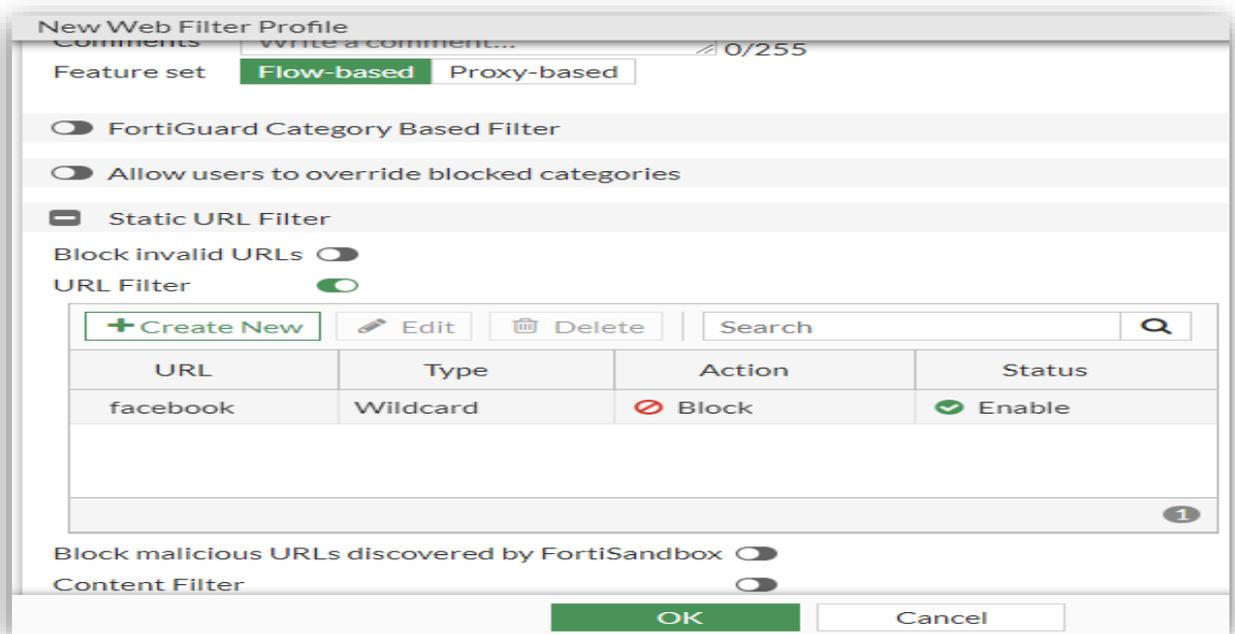


Figure 4.30 : Création d'URL Facebook

➤ Attacher le profil de sécurité à la politique de Fortigate

Après avoir créé le filtre d'URL, nous devons l'attacher à une stratégie de Fortigate que l'on a déjà créé **Figure 4.25**.

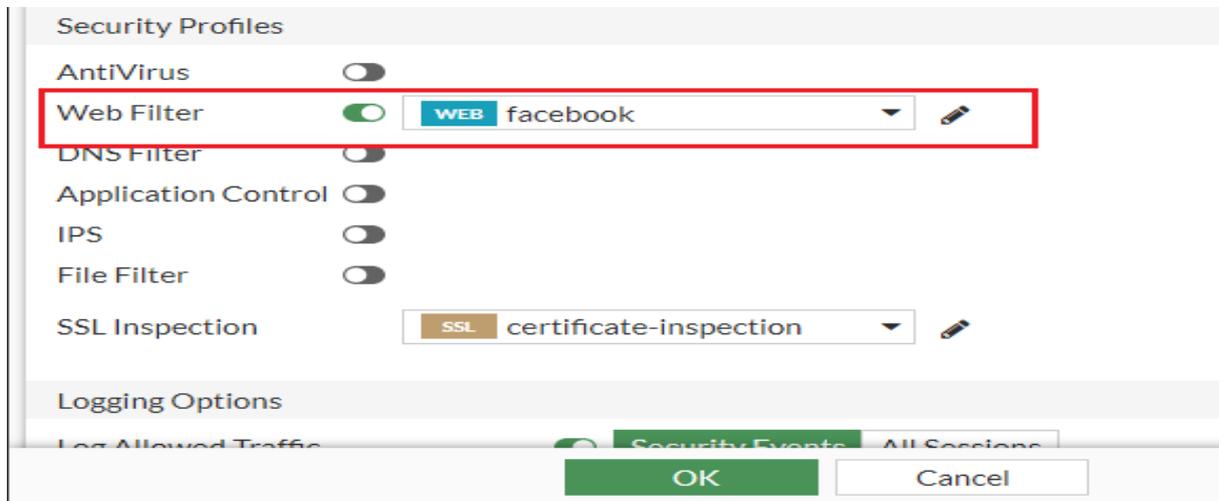


Figure 4.31 : Bloquer Facebook

➤ Valider les résultats du filtre d'URL

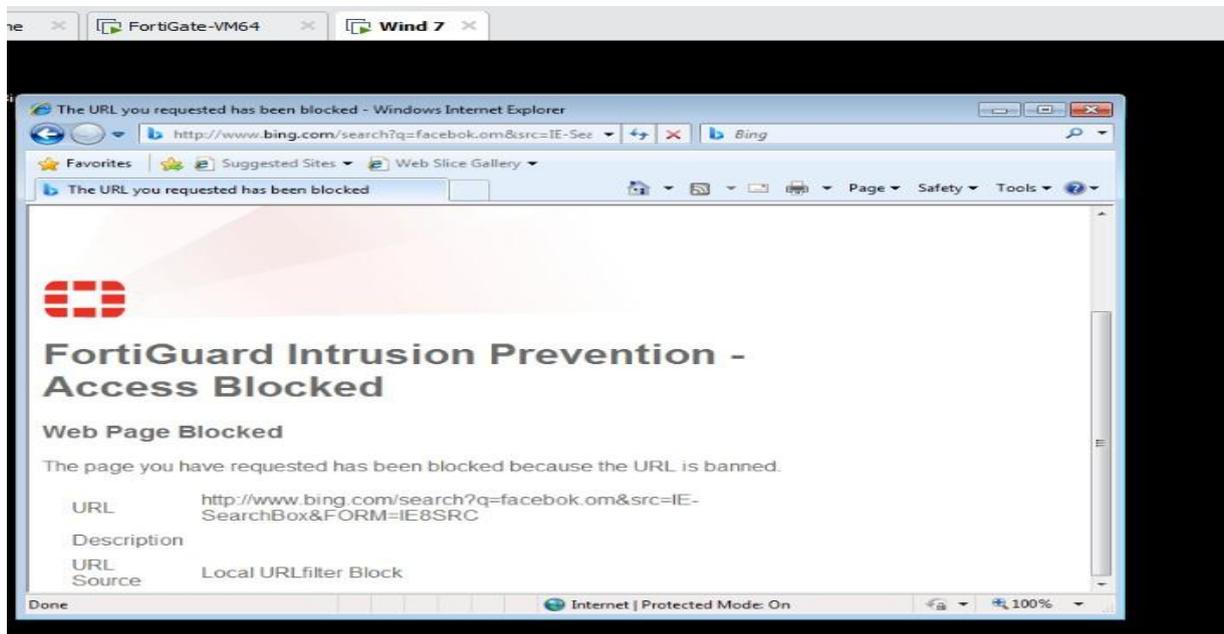


Figure 4.32 : Local URL Filter block

4.3.3. Configurer la DMZ sur le pare-feu FortiGate

La DMZ est similaire au LAN, tandis que le réseau LAN utilise principalement l'accès sortant du LAN vers Internet. Dans le cas de la DMZ, le trafic sera entrant d'Internet vers le côté DMZ, ou du côté LAN vers la DMZ. Il faut toujours conserver les serveurs connectés à Internet sur la DMZ. Il peut s'agir de serveurs Web, de serveurs de messagerie, de serveurs FTP/SFTP, etc.

Nous avons déjà configuré le côté LAN ainsi que le côté WAN. Maintenant, nous allons configurer un réseau DMZ dans le pare-feu Fortigate.

- **Création de la machine virtuelle (Windows serveur2016)**

Pour faire fonctionner le serveur 2016 nous avons besoin d'une image iso. Nous devons simplement la télécharger sur le lien suivant <https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2016>

Après avoir téléchargé l'image ISO de Windows Server 2016, nous avons créé une machine virtuelle sous « VMware workstation15 » sous le nom win2016.

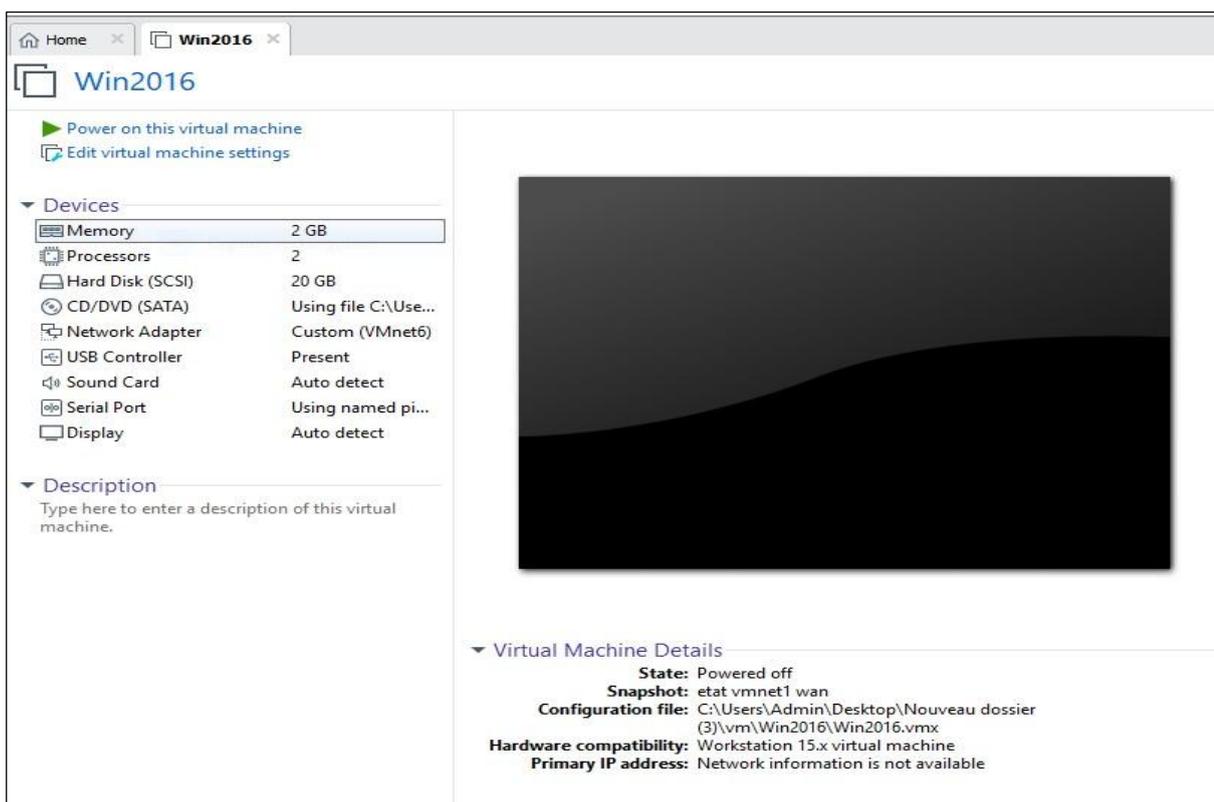


Figure 4.33 : Machine virtuelle de Windows serveur 2016

Pour commencer l'installation du serveur, nous cliquons sur **power on this virtual machine**.

Après quelques secondes, nous arrivons à l'écran suivant (**Figure 4.34**), nous choisissons les valeurs pour chaque entrée affichée dans l'image puis nous cliquons sur « suivant ».

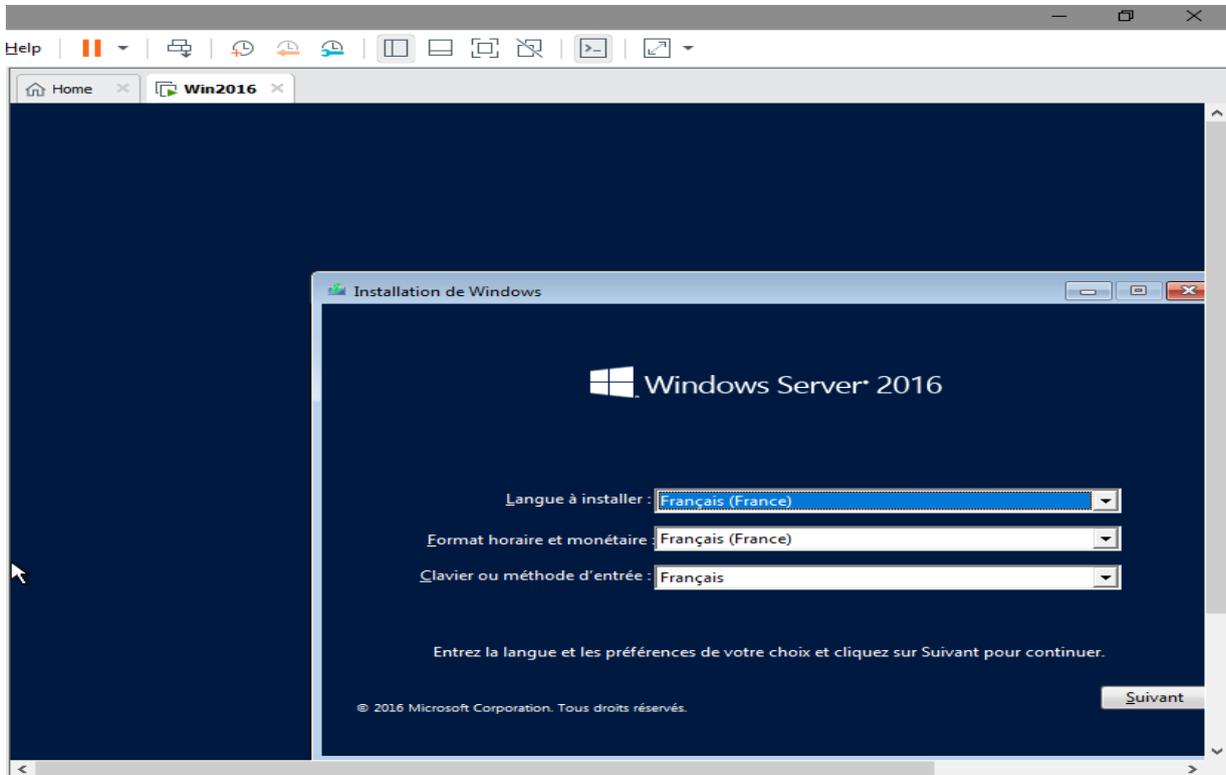


Figure 4.34: Ecran de l'installation de Windows serveur

Après avoir cliqué sur « Suivant », nous cliquons à nouveau sur « Installer Maintenant » pour lancer l'installation.

Une fois avoir cliqué sur « Installer maintenant » Nous allons passer à la sélection du système d'exploitation à installer (**Figure 4.35**). En ce qui nous concerne, nous installerons la version 2 qui utilise l'interface graphique de Windows.

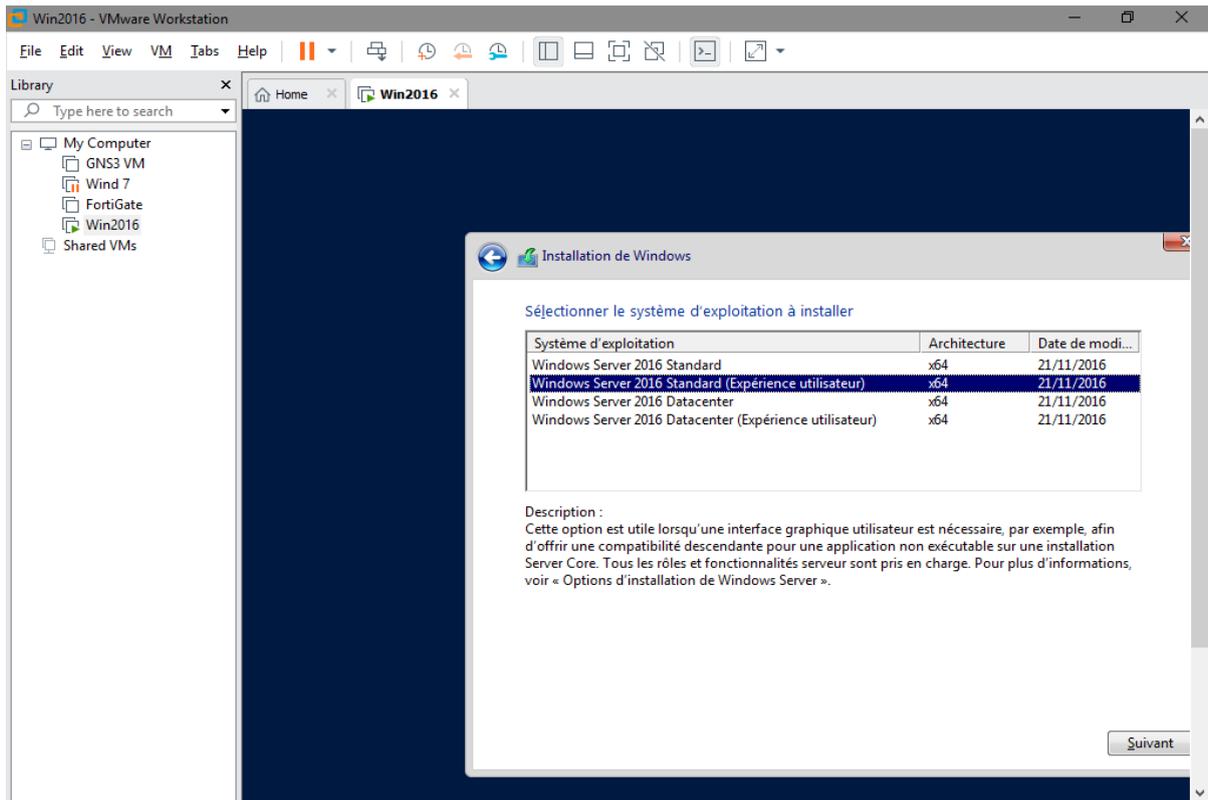


Figure 4.35 : Edition du système d'exploitation

Nous cliquons sur suivant puis nous acceptons les termes de licence. Ensuite nous passons à la sélection du type d'installation (Figure 4.36).

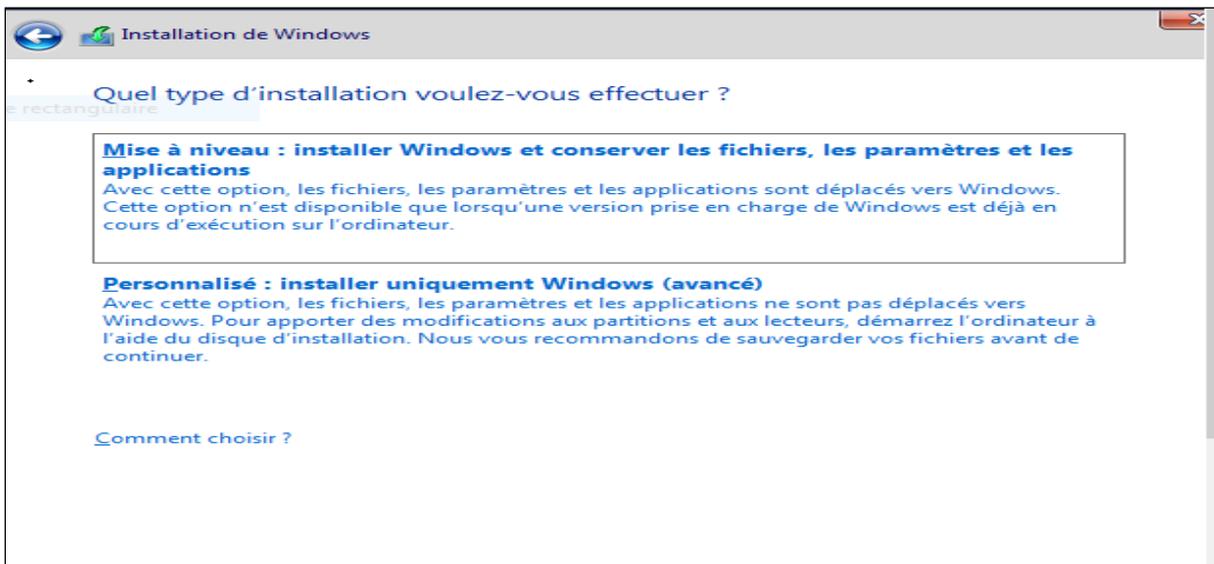


Figure 4.36 : Type d'installation de Windows

L'image ci-dessous illustre la sélection de l'emplacement où nous voulons installer le système d'exploitation. Comme nous avons choisi un seul disque lors de la création de la machine virtuelle, un seul disque s'affiche ici.

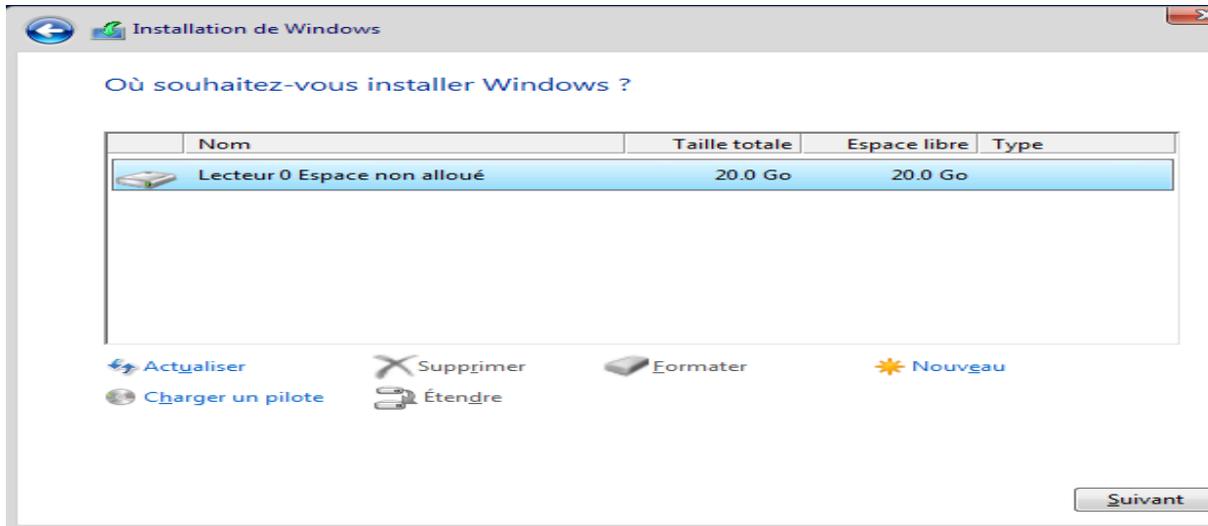


Figure 4.37 : Emplacement de l'installation de Windows

L'installation va maintenant démarrer. Une fois l'installation de Windows serveur terminée. Celui-ci lance une première fois les paramètres de notre compte d'utilisateur (administrateur) du serveur, nous tapons un mot de passe et appuyons sur Entrée pour nous connecter à la machine.

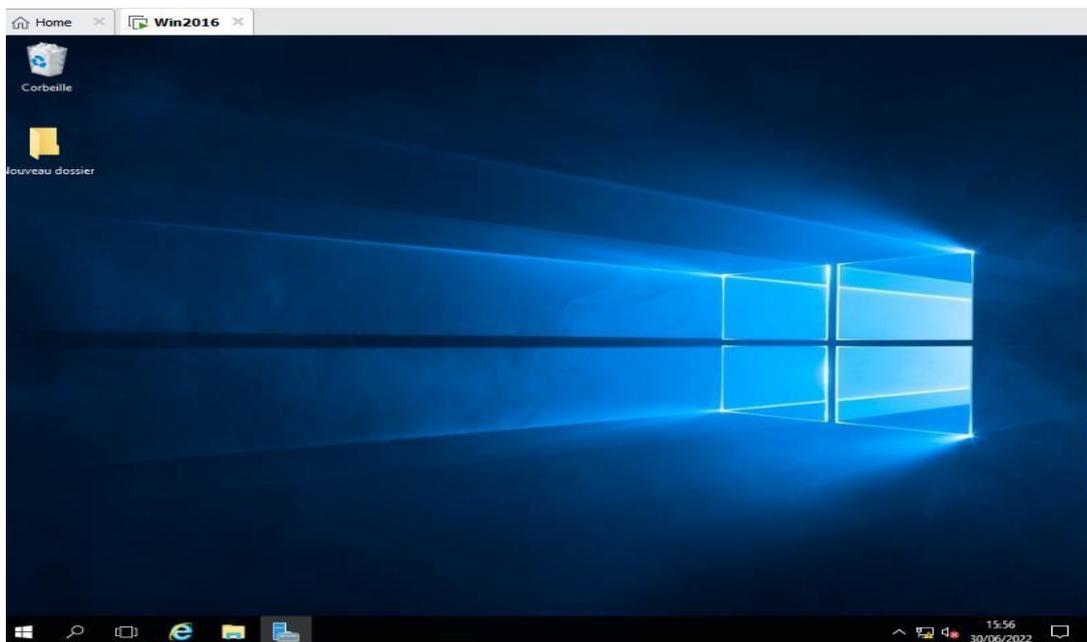


Figure 4.38 : Ecran d'accueil de Windows serveur

➤ Héberger un site Web à l'aide d'IIS dans Windows Server 2016

• Activer le service IIS dans Windows 2016

- 1) Sur le bouton démarrer de Windows->Gestionnaire de serveur -> ajouter des rôles et des fonctionnalités->suivant.
- 2) Nous sélectionnons **Installation basée sur un rôle ou une fonctionnalité** ->suivant.
- 3) Nous sélectionnons le serveur approprié. Le serveur local est sélectionné par défaut ->Suivant.
- 4) Activer **Serveur Web (IIS)** -> Suivant.
- 5) Aucune fonctionnalité supplémentaire n'étant nécessaire à l'installation de l'adaptateur Web, nous cliquons sur Suivant.
- 6) Dans la boîte de dialogue **Rôle Serveur Web (IIS)**, nous cliquons sur **Suivant**.
- 7) Dans la boîte de dialogue **Sélectionner les services de rôle**, nous avons choisi l'option **serveur Web**, cela garantira l'installation d'IIS puis nous cliquons sur **Suivant**.
- 8) Dans l'écran final, nous cliquons sur **Installer** pour commencer l'installation.
- 9) Au terme de l'installation, nous cliquons sur Fermer pour quitter l'assistant.

• Créer un nouveau site Web

Sur le bouton démarrer de Windows ->gestionnaire de serveur->outil ->gestionnaire des services internet (iis), nous cliquons sur Sites -> Ajouter un site Web

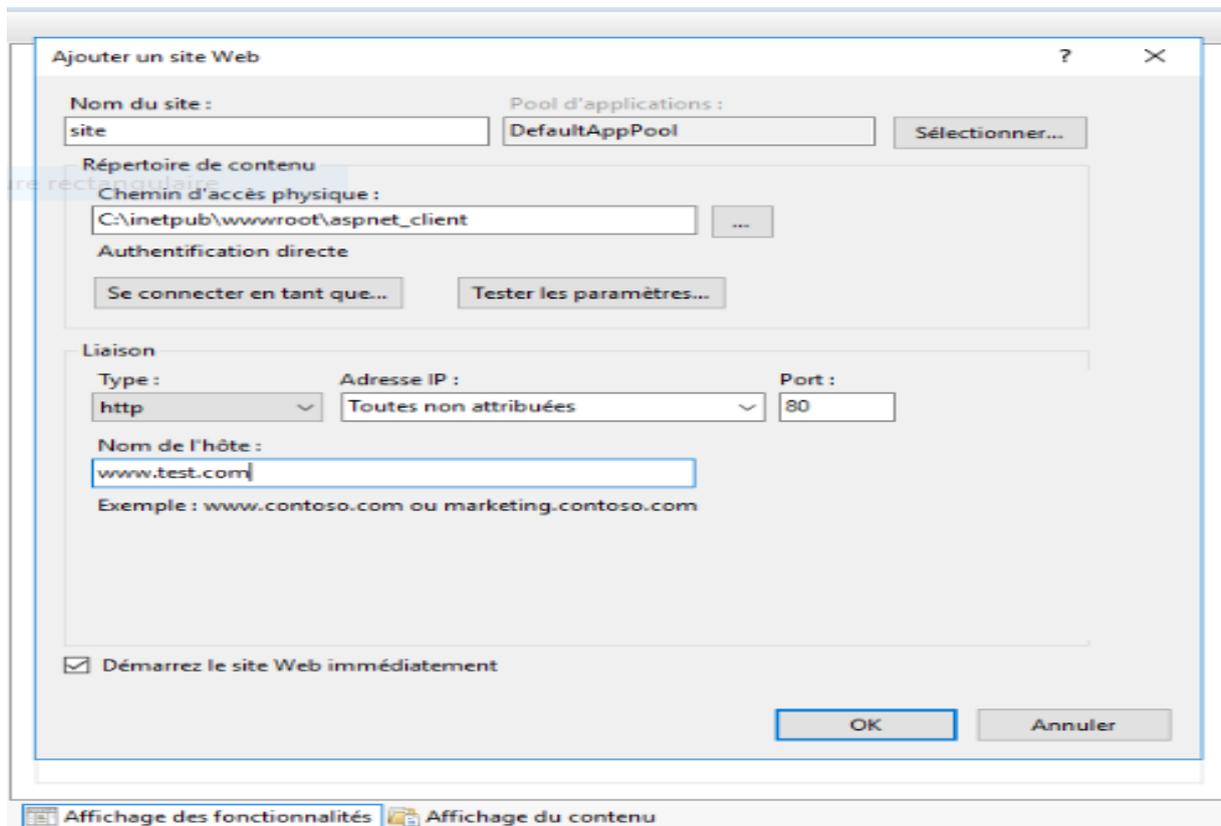


Figure 4.39 : Création d'un site web

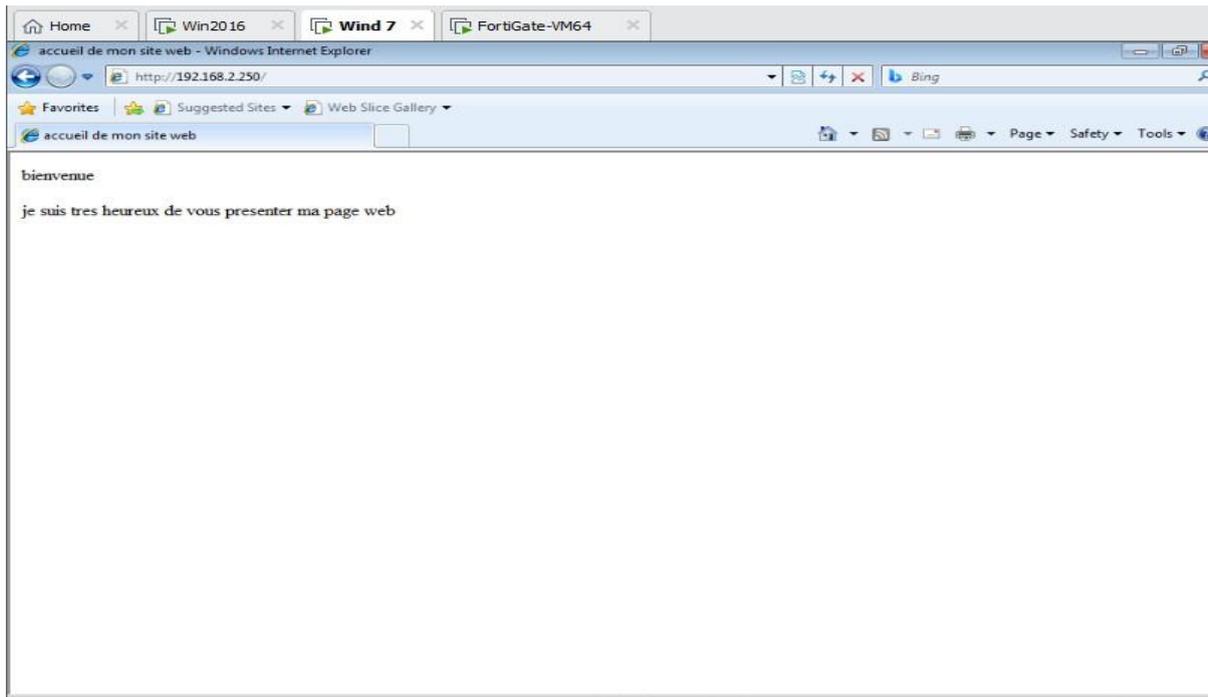


Figure 4.40 : Interface de notre site web

➤ Configuration de l'interface DMZ

Nous allons introduire ici un réseau DMZ 192.168.2.0 /24, pour ce faire il faut se rendre dans **Network->Interfaces->port3**, puis un clic droit et nous cliquons sur **Edit**. Nous devons configurer l'adresse IP manuellement sur le serveur. Dans une DMZ, nous n'activons généralement pas le service DHCP.

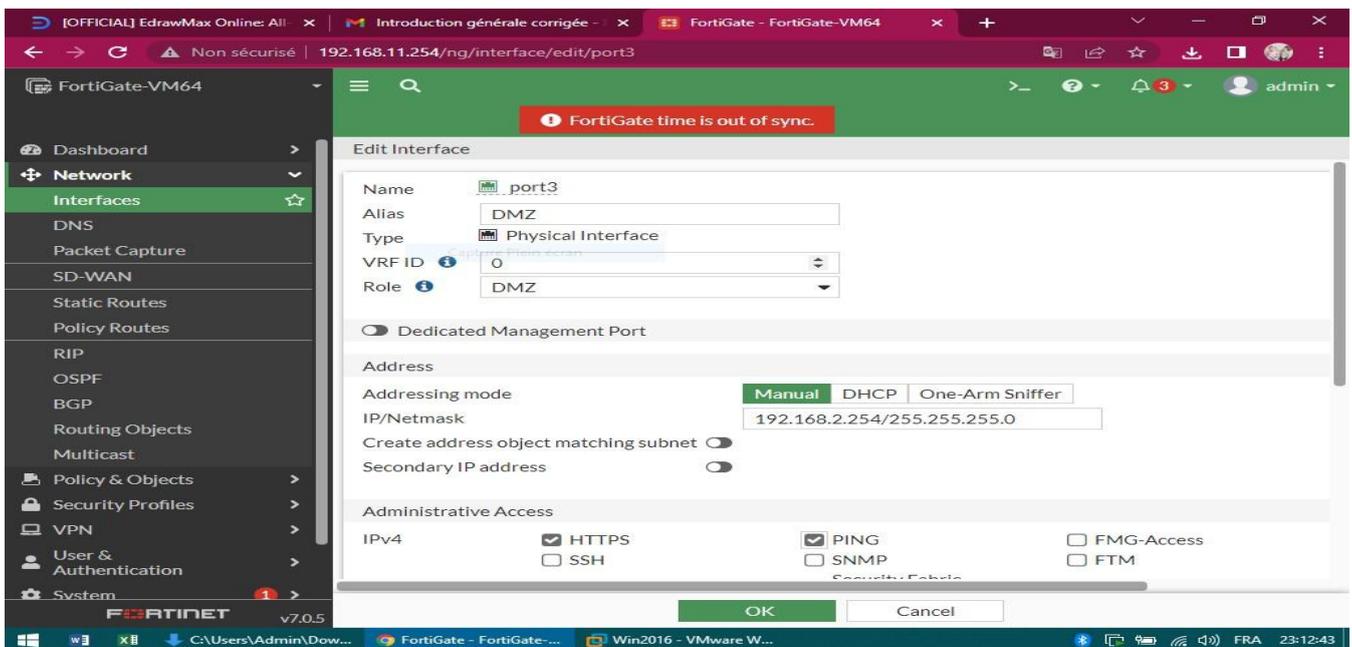


Figure4.41 : Configuration de l'interface DMZ

Nous cliquons ensuite sur le bouton Démarrer de **Windows** ->**Virtual Network Editor**, nous utilisons donc l'adaptateur VMnet6 comme « host-only ». Après cela, nous devons fournir une adresse IP.

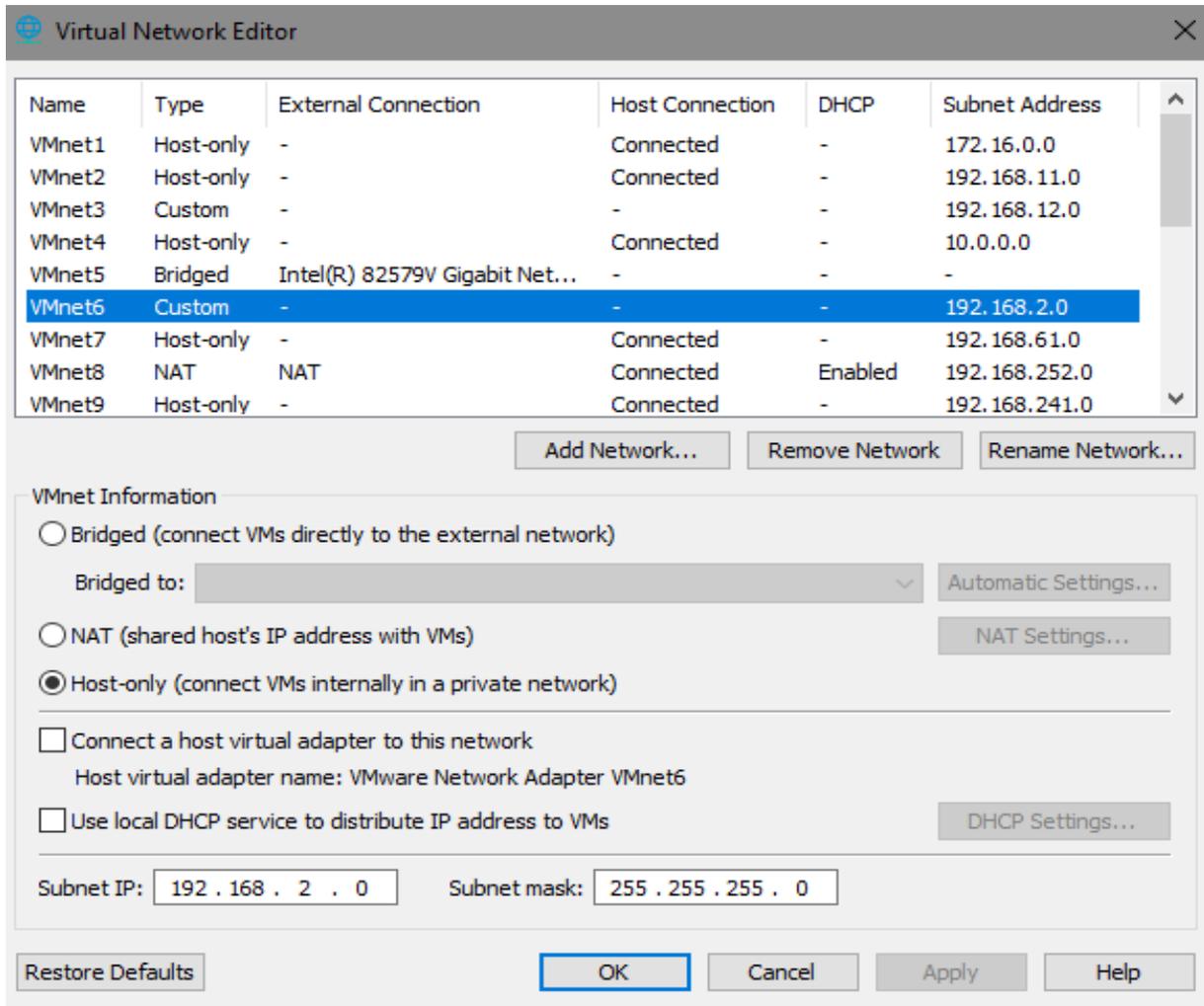


Figure 4.42 : Configuration de l'interface DMZ coté VMware

Connecter le serveur Web au commutateur

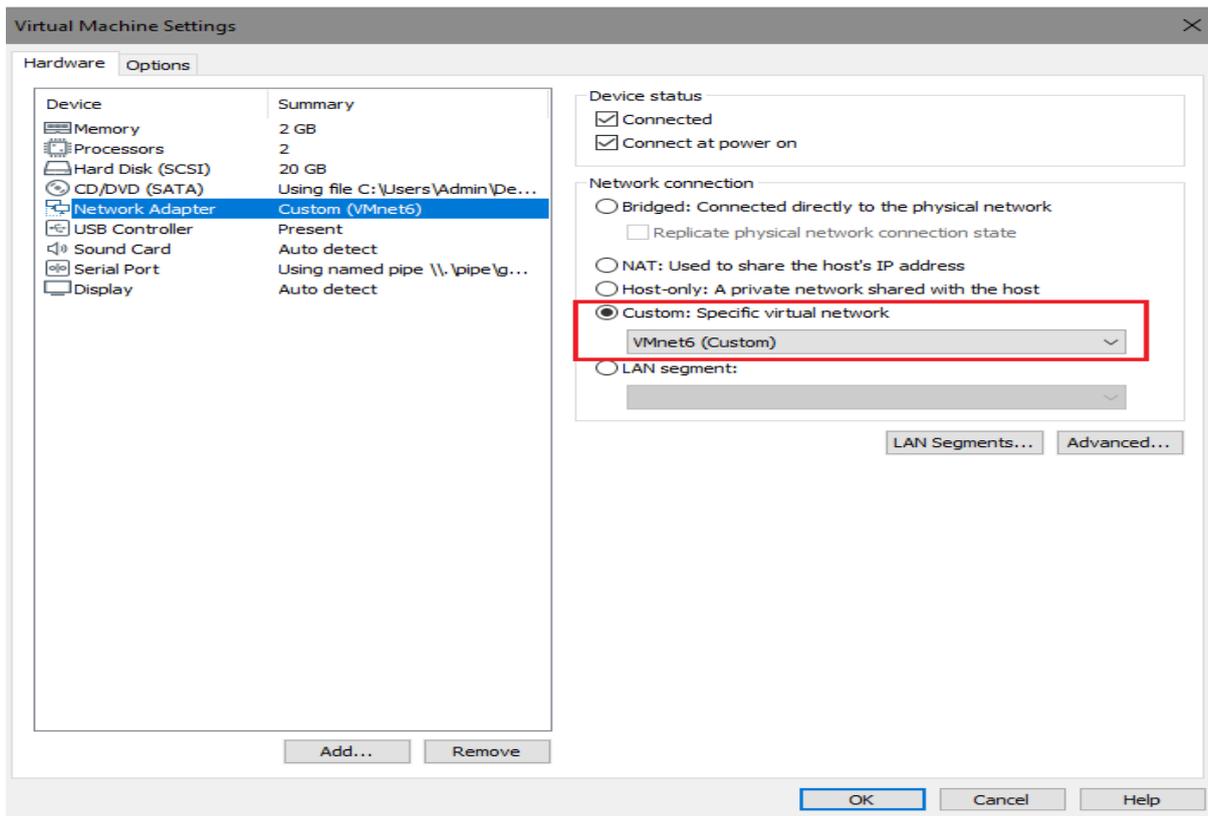


Figure 4.43 : Connecter le serveur au commutateur

Configurer l'adresse IP manuellement sur le serveur.

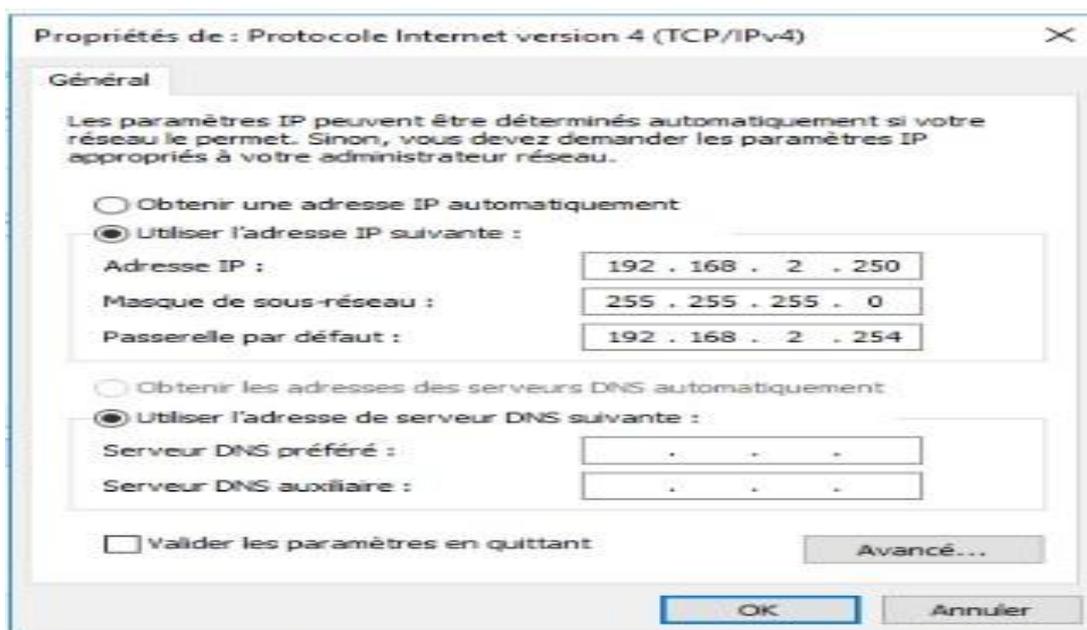


Figure 4.44 : Ecran de configuration de la carte réseau du serveur

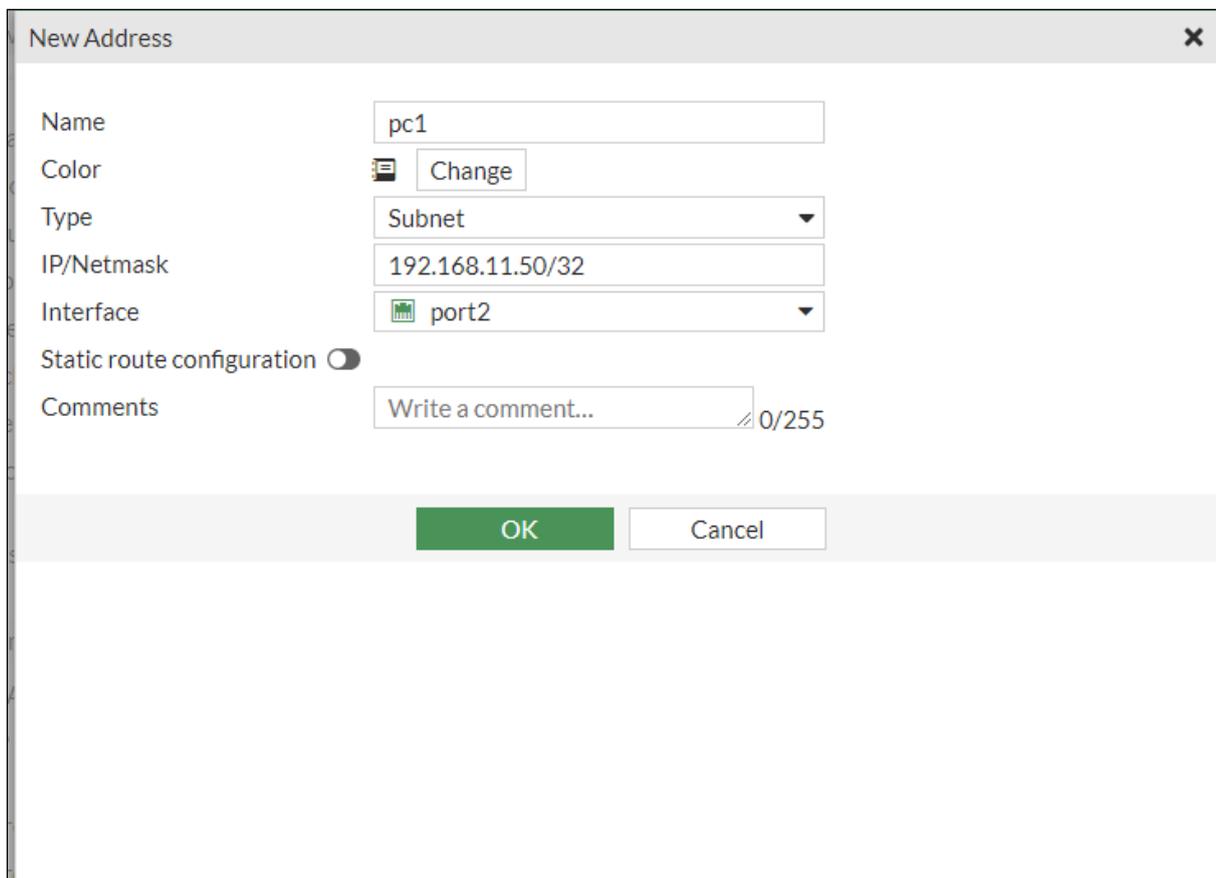
➤ **Activer la communication entre le LAN et la DMZ**

Tout trafic entrant/sortant de la DMZ est bloqué parce que nous n'avons aucune politique. Nous configurons la politique de sécurité et permettons au réseau LAN d'atteindre le serveur HTTP.

- **Création des adresses objets**

Avant de continuer et de créer une politique, nous créons des objets Adresses, que l'on peut appeler ultérieurement dans la création de la politique. Nous nous rendons dans :

Policy&Objects ->Addresses ->Create New->Address.



The image shows a 'New Address' dialog box with the following fields and values:

- Name: pc1
- Color: Change
- Type: Subnet
- IP/Netmask: 192.168.11.50/32
- Interface: port2
- Static route configuration:
- Comments: Write a comment... 0/255

Buttons: OK, Cancel

Figure 4.45: Création de l'adresse objet du PC LAN

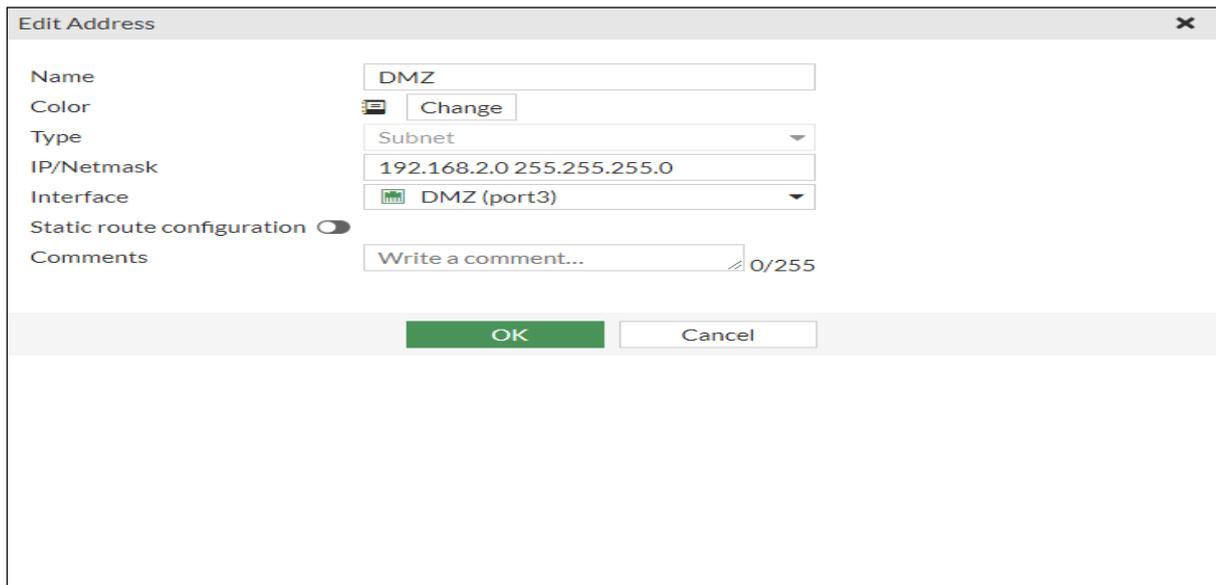


Figure 4.46 : Création de l'adresse objet DMZ

➤ **Création d'une politique**

Nous allons créer une politique de sécurité pour permettre au réseau LAN d'atteindre le serveur. Nous nous rendons dans : **Policy&Objects-> Firewall Policy->Create Policy**

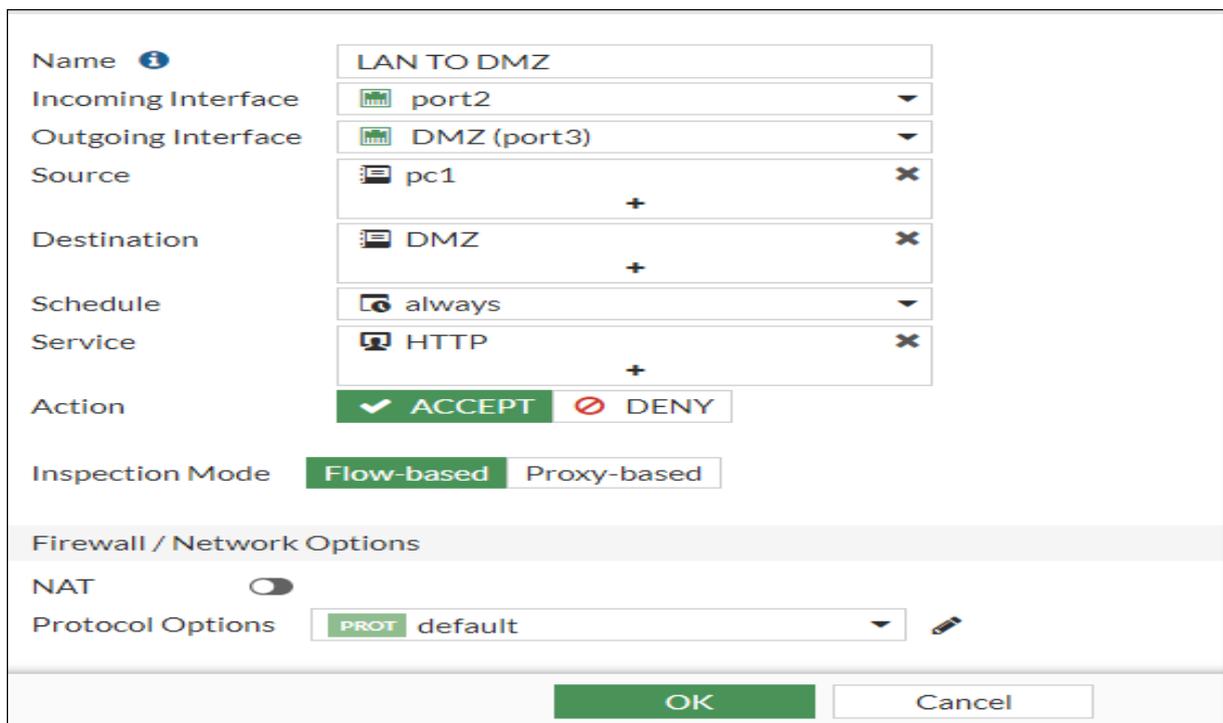


Figure 4.47: Création de la politique LAN vers DMZ

- Teste de connectivité
 - Client → serveur

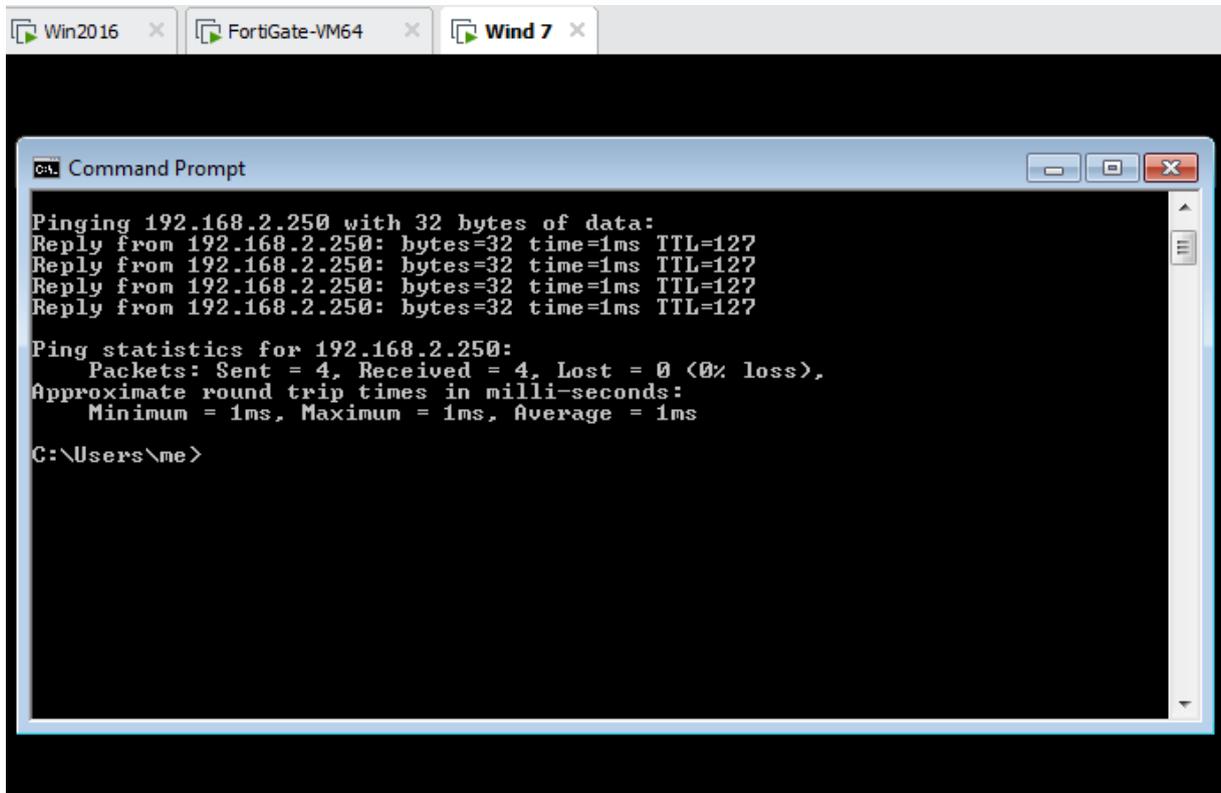


Figure 4.48: Ping de la machine client vers le serveur

Nous essayons d'accéder au serveur Web à partir du réseau local

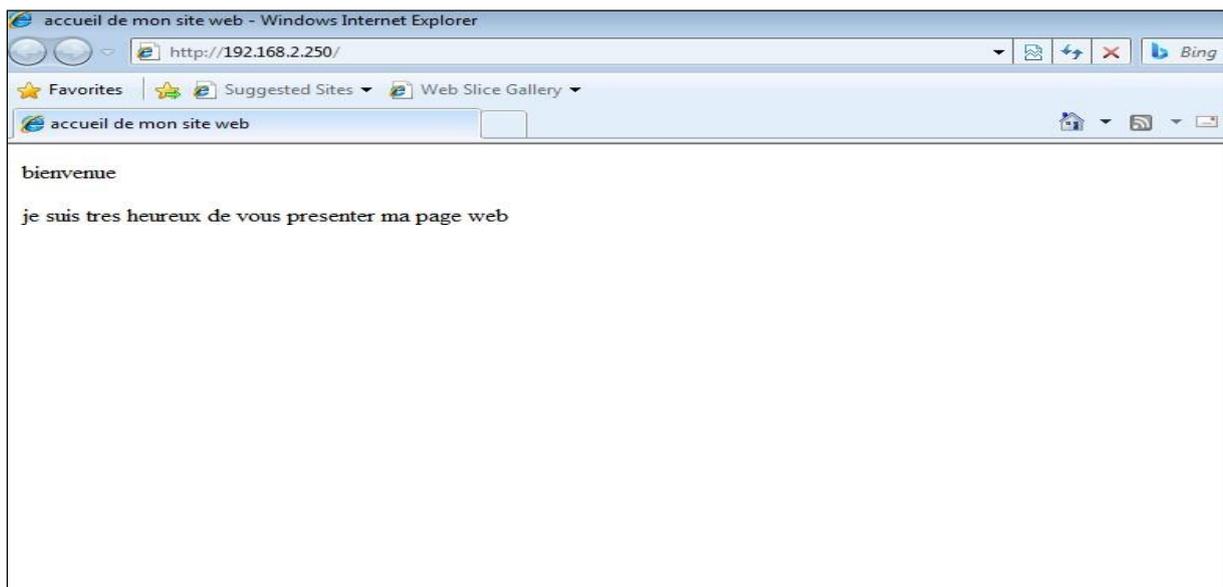


Figure 4.49 : Accueil de site web du serveur

Conclusion

Dans ce chapitre, nous avons mis en œuvre les solutions que nous avons proposées pour notre problématique, et ce à travers la réalisation d'un Fortigate, ainsi qu'un aperçu de quelques étapes de son installation, sa configuration et les différentes règles de filtrage.

Conclusion Générale

Il existe un très grand nombre d'attaques possibles sur les réseaux informatiques. Parmi les solutions potentielles contre ces attaques, Fortigate est un des éléments pouvant être mis en place dans le cadre d'une politique de sécurité définie. En effet, il peut s'avérer être très utile et très efficace si celui-ci est bien configuré, notamment dans le domaine du contrôle des flux de données.

FortiGate est un composant réseau qui permet non seulement de concentrer l'administration de la sécurité en des points d'accès limités au réseau d'entreprise, mais aussi de créer un périmètre de sécurité, par exemple entre le réseau intranet de l'entreprise et le réseau Internet, il faut pour cela activer tous les services de Fortigate (IPS/IDS, antivirus, antispam, filtrage web, etc.). Ces derniers constituent les éléments essentiels d'une politique globale de sécurité.

L'objectif principal de notre travail a été la réalisation d'un système de sécurisation pour le réseau de l'entreprise d'accueil, et la mise en place d'un Firewall (Fortigate) qui permet une protection efficace contre les attaques qui viennent de la part des pirates informatiques.

Ce travail nous a permis d'enrichir nos connaissances dans le domaine de la sécurité des réseaux, et notamment « Fortigate » et certains outils et logiciels ainsi que leur fonctionnement et leur rôle dans la sécurité des entreprises.

Finalement, nous espérons que notre travail sera bénéfique pour la sécurité de l'entreprise d'accueil.

Bibliographie

- [1] : M. YAZID. Support de cours, Réseaux informatique ,2016 /2017.
- [2] : JF.Pillou,F.LEMAINQUE. Tout sur les Réseaux et Internet. 4ème édition Dunod ,2012 ,2015.
- [3] : L.Tahtat , Z.Bensafia.Installation et configuration de pare-feu pfsense au sein de l'entreprise Ramdy , Université de bejaia ,2019/2020.
- [4]: boucherba khadiidja,Ziane saloua .mise en place d'un pare-feu d'entreprise open source pfsense,université de bejaia, 2015.
- [5] : préface de Michel, solange Ghrnaouti-Hélie. Sécurité informatique et Réseaux.2ème édition.
- [6] : Le Grand Livre de Securiteinfo.<http://www.securiteinfo.com> ,19 février 2004.
- [7] : JF.pillou, JF bay, sécurité informatique.3^{ième} édition,Dunod, paris 2013.
- [8] :H.Alim, M.Ourabah, Mise en place et déploiement du pare-feu PFsense ,HIMI-bejaia , 2015/2017 .
- [9]:JF.pillou, JPH.Bay.tout sur la sécurité informatique .4ème édition Dunod ,2005.2009.2013.2016 .

Webographie

- [10]: www.bejaiamed.com
- [11]: <https://www.fortinet.com>
- [12]: <https://www.fortinet.com/resources/cyberglossary/unified-threat-management>
- [13]: <https://www.comparatif-logiciel.fr/logiciel/fortigate-vm>
- [14]: [HTTPS://www.lebigdata.fr/windows-server-tout-savoir](https://www.lebigdata.fr/windows-server-tout-savoir)

Résumé

Durant la dernière décennie, le réseau informatique mondial Internet a connu une croissance exponentielle. En effet, il permet d'échanger de très grandes quantités d'informations dans des délais extrêmement courts, ce qui permet, notamment, d'augmenter la productivité des entreprises. Cependant, le raccordement de ces dernières au réseau mondial impose toute une politique de sécurité au niveau de l'entreprise qui s'y connecte, et des protections matérielles et logicielles suffisantes pour éviter tout risque de fuites ou piratage.

Dans notre mémoire, nous nous sommes intéressés à la sécurité réseau à base d'une stratégie de sécurité qui s'appuie sur Fortigate, pour pouvoir sécuriser au maximum le réseau de l'entreprise BMT (Bejaia Méditerranéen terminal) contre les menaces et les attaques éventuelles qui risquent de l'atteindre.

Mots clés : Réseaux informatiques, Sécurité réseau, Fortigate, Filtrage de paquets, LAN, WAN, DMZ

Abstract

During the last decade, the internet knew an exponential increase. In fact, it allows exchanging huge quantity of information within extremely small periods, which permits increasing the productivity of the companies. However, the connection of the latter to the network imposes a whole security policy on the company level which it is connected to, and sufficient materiel and software protections to avoid any risk of hacking.

In our work, we were interested in network security based on a security strategy which involves Fortigate, in order to be able to secure as much as possible the network of the BMT company (Bejaia Mediterranean terminal) against the threats and possible attacks that may reach it.

Keywords: Computer networks, Network security, Fortigate, Packet filtering, LAN, WAN, DMZ.