République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la

Recherche Scientifique Université Akli Mohand

Oulhadj –Bouira-

Faculté : *Sciences et Sciences Appliquées*

Département : *Génie Electrique*

Domaine : *Sciences et Technologie*

Filière : *Télécommunication*

Spécialité : *systèmes des télécommunications*

Mémoire de fin d'études
Pour l'obtention du diplôme de MASTER

Thème :

Mise en place d'un réseau LAN sécurisé du système VSAT via FortiGate

Réalisé par :

- DERMECHE Narimane
- MEZYENE Thanina

Encadré par :

- MEDJDOUB Smail M.A.A

Devant le Jury composé de :

• BOUGHAROUAT Ali	M.C.B	Président
• ASRADJ Zouhir	M.C.A	Examinateur

2020/2021

Remerciements

Nos vifs remerciements vont :

A Dieu le tout puissant qui, par sa grâce, nous a permis d'arriver au bout de nos efforts en nous donnant la santé, la force, le courage et en nous faisant entourer des merveilleuses personnes que nous remercions.

A toutes celles et tous ceux qui nous ont enseigné depuis notre entrées à l'école à ce jour.

A toutes personnes qui nous a encouragé et aider à suivre cette formation et à réaliser ce présent mémoire.

Dédicaces

Louange à dieu tout puissant, qui m'a permis de voir ce jour tant a attendu.

Je dédie ce mémoire

A ma tendre Mère

La lumière de mes jours, la source de mes efforts, la flamme de mon cœur, ma vie et mon bonheur ma maman chérie que j'adore.

A mon très cher Papa

Le guide de mes désirs, le donneur avec plaisir, à toi ma fierté et mon pouvoir,

Merci.

A la mémoire de mon ***grand père*** *et* ***ma grand-mère****, que dieu les accueils dans son vaste paradis.*

A ma très chère ***sœur*** *et mon cher* ***frère****.*

A mon mari ***Kamel***

A mes tantes et mes cousines.

A ma petite cousine ***MARAM****.*

À Mon binôme ***Thanina*** *avec qui j'ai partagé la fatigue et les bons moments durant cette période de travail.*

À tous ce que j'aime et qui m'aiment.

À tous mes amis.

Narimane.

Dédicaces

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.

Ce modeste travail est le fruit de tous les sacrifices que vous avez fait pour mon éducation et ma formation. Je vous aime énormément je pris le tout-puissant pour qu'il vous accorde une bonne santé et une vie longue et heureuse.

A mes chers frères ***Jugurtha*** *et* ***Moussa****, ma chère sœur* ***Lahna****, et ma belle sœur* ***Ouiza*** *sans oublier mon petit ange* ***Anir****, qui m'ont toujours soutenu et encouragé durant ces années d'études par leurs tendresses, complicités et présences.*

À Mon binôme ***Narimane*** *avec qui j'ai partagé la fatigue et les bons moments durant cette période de travail.*

A tous mes amis.

Que dieu vous donne santé, bonheur, courage, et surtout réussite.

Thanina.

Table des matières

Chapitre I: Notions de base sur les réseaux informatiques

Chapitre II: Sécurité de réseau LAN

Chapitre III: Déploiement d'un réseau LAN protégé par Fortigate

Liste des figures

Chapitre I: Notions de base sur les réseaux informatiques

Chapitre II: Sécurité de réseau LAN

Chapitre III: Généralité sur les systèmes VSAT

Liste des tableaux

Chapitre I: Notions de base sur les réseaux informatiques

Chapitre III: Déploiement d'un réseau LAN protégé par Fortigate

Liste des abréviations

ACK : Accusé de réception

AED: Network Anomaly Detection Engines

AIS: Automatic Identification System

ANSI: American National Standards Institute

ARPANET: Advanced Research Projects Agency Network

ASIC: Application Specific Integrated Circuit

BYOD: Bring Your Own Device

CRC: Cyclic Redundancy Check

CSMA/CD: Carrier Sense Multiple

DDoS : Distributed Denial of Service

DHCP: Dynamic Host Configuration Protocol

DMZ: Demilitarized Zone

DNS: Domain Name System

EVE_NG: Emulated Virtual Environment _Next Generation

FTP: File Transfer Protocol

GUI: Graphical User Interface

HTTP: Hypertext Transfer Protocol

ICMP: Internet Control Message Protocol

IDS: Intrusion Détection System

IEEE: Institute of Electrical and Electronics Engineering

IETF: Internet Engineering Task Force

IP: Internet Protocol

IPS : Index de Pression Systolique

IPSI: Système de Prévention des Intrusion

ISOC: Internet Society

ITU: Union Internationales des Télécommunications

LAN: Local Area Network

LDPC: Low-density Parity-check

LED: Light – emitting Diode

LOGS: Logging

MAN: Metropolitan Area Network

MILNET: Fully Military Network

MitM: Man-in-the-Middle

MODEM: Modulateur / Démodulateur

MPLS : Multiprotocol Label Switching

NAT: Traduction d'Adresse Réseau

NET BIOS/SMB: Network Basic Input Output System / Server Message Block

NGFW: Firewall Nouvelle Generation

NP7: Network Processor 7

OSI: Open System Interconnection

OSPF: Open Shortest Path First

PDU : Unité de Données de Protocole

RAM : Random Access Memory

RFC: Requests for Comments

RIP: Routing Information Protocol

RST: Reset

SQL: Structured Query Language

SMTP: Simple Mail Transfer Protocol

SSL: Secure Socket Layer

SPAIN: Switched Port Analyzer

SPU: Security Processing Unit

SYN-ACK : Synchronize-acknowledge

SYN : Synchronisation

TCP/IP: Transmission Control Protocol/ Internet Protocol

TCP_SYNC : Three-way-Handshake

TLS1.3: Sécurité de la Couche de Transport

UDP: User Datagram Protocol

URL: Uniform Resource Locator

USB: Universal Serial Bus

VLAN: Réseau Local Virtual

VPC: Virtual Private Cloud

VPN: Virtual Private Network

VSAT: Very Small Aperture Terminal

WAN: Wide Area Network

Introduction générale

Introduction générale

L'accroissement des trafics en télécommunication révèle les besoins grandissants d'échanges de données que ce soit dans le domaine privé ou professionnel.

La sécurité réseau est devenue un sujet de recherche très intense. Ces recherches ont permis le développement de certains dispositifs de protection des systèmes informatiques et des réseaux tels que les pare-feux, l'antivirus, détecteur des anomalies, ...etc.

Dans le cadre de notre projet de fin d'études nous avons effectué un stage au sein d'Algérie Télécom Satellite (ATS). L'objectif est d'étudier la sécurité d'un réseau LAN du système VSAT via FortiGate.

La solution de sécurité proposée repose sur l'utilisation de FortiGate NGFW. Ce dernier est un système permettant de protéger un réseau des intrusions. Ce système permet de maîtriser les coûts et de les simplifier, inspecter le trafic réseau entrant et sortant, communiquer avec toutes les solutions soit dans Fortinet ou dans un environnement hétérogène. Il est une alternative au déploiement de plusieurs outils autonomes combinés dans une seule plateforme.

Le présent mémoire est formé de trois chapitres :

- Le premier chapitre est consacré aux généralités sur les réseaux et la sécurité informatique.
- Dans le deuxième chapitre, nous avons présenté les Firewalls, leurs principes de fonctionnement et les attaques.
- Le troisième chapitre décrit la solution étudiée et son exploitation. Dans la dernière partie on retrouve les tests de bon fonctionnement de la solution et ses résultats.

Chapitre I :

Notion de base sur les réseaux informatiques

I. Introduction

Les réseaux sont nés du besoin d'échanger des informations de manière simple et rapide entre des machines. Au début, toutes les informations étaient centralisées dans une seule machine, c'est le mode **autonome.**

Vu l'augmentation du besoin de ces informations par les utilisateurs et les programmes et pour des raisons de coûts et de performances, on a multiplié le nombre de machines.

Les informations devaient être dupliquées sur les différentes machines du même site qui sont reliées entre elles par des câbles. Ce fût l'apparition des réseaux moyens et des réseaux de longues distances.

Aujourd'hui, les réseaux se trouvent à l'échelle planétaire. Comme le besoin d'échange de l'information évolue du jour en jour, ce fût l'apparition du réseau mondial (Internet).

I.1. Définition d'un réseau informatique [1]

Un réseau informatique est un réseau dont chaque nœud est un système informatique autonome, interconnecté afin de communiquer (émission/réception) par l'intermédiaire d'un support de communication. Il existe deux types de réseaux : le réseau filaire et le réseau sans fil.

I.2. Buts des réseaux informatiques [1]

Les réseaux informatiques permettent :

- Le partage des fichiers et d'applications.
- La communication entre les personnes (courrier électronique, discussion en direct …).
- La garantie de l'unicité de l'information (base de données).
- Réduire les coûts (partages des ressources matérielles et logicielles).

I.3. Topologies des réseaux informatiques [2]

Une topologie décrit la manière dont les équipements réseaux sont interconnectés et reliés entre eux grâce à des matériels (câblage, cartes réseaux, …). Ce type de topologie est appelé la topologie physique. Il existe un autre type qui s'appelle la topologie logique qui décrit la manière dont transitent les informations.

I.3.1. Topologie physique

Parmi les topologies physiques, les plus connues sont :

I.3.1.1.Topologie en bus : Dans cette topologie tous les ordinateurs sont liés directement à une liaison centrale par l'intermédiaire de câble coaxial.

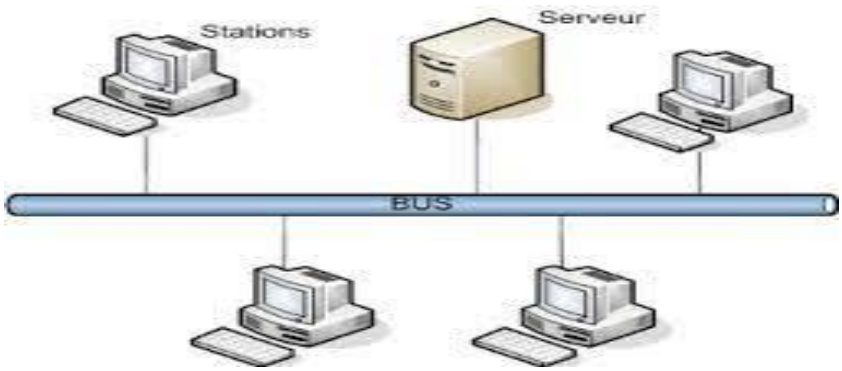

Figure I.1 : Topologie en bus.

I.3.1.2.Topologie en anneau : Dans cette topologie, tous les ordinateurs sont reliés directement à une liaison centrale en boucle, les communications sont monodirectionnelles.

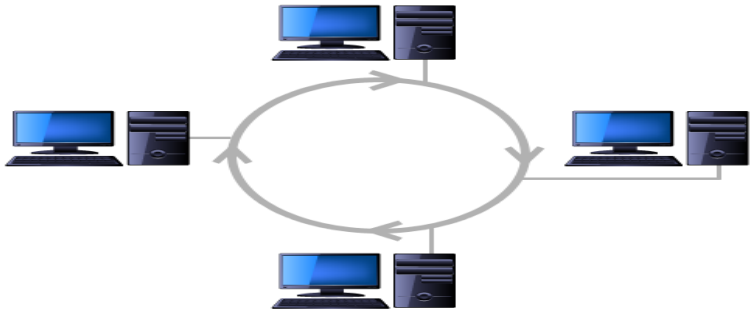

Figure I.2 : Topologie en anneau.

I.3.1.3.Topologie en étoile : Dans cette topologie, tous les ordinateurs sont reliés à un système central appelé HUB ou concentrateur. Le réseau est limité par les possibilités du HUB (N-1 liaison pour N ordinateurs).

Figure I.3 : Topologie en étoile.

I.3.1.4.Topologie hybride : Dans un réseau de grande taille on utilise la topologie hybride. Qui est un mélange de différentes topologies en bus, en anneau et en étoile.

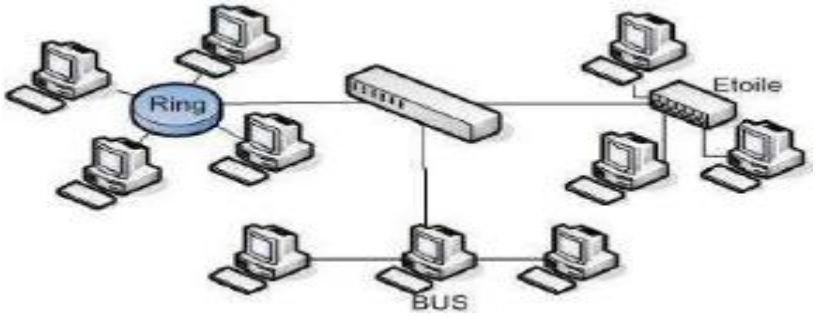

Figure I.4 : Topologie hybride.

I.3.1.5.Topologie maillée : Dans cette topologie, on utilise des connexions point à point entre toutes les unités.

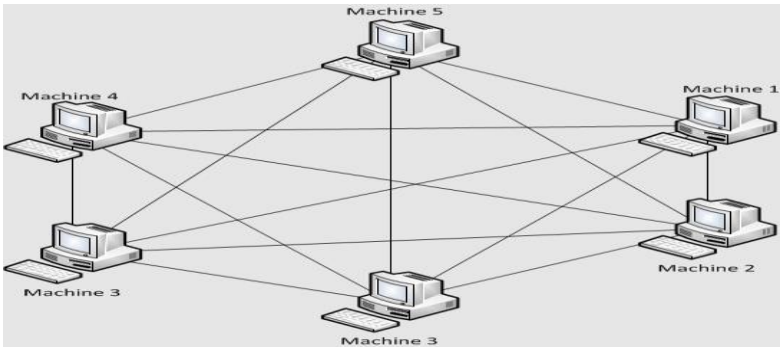

Figure I.5 : Topologie maillée.

I.3.1.6.Avantages et inconvénients de topologie physique

Pour choisir la topologie qui répondra le mieux à nos besoins, on doit prendre en considération les facteurs suivants :

Topologies	Avantages	Inconvénients
Bus	• Economie de câblage. • Support économique et facile à manipuler. • Système simple et fiable.	• Ralentissement possible du réseau lorsque le trafic est important. • Problèmes difficiles à isoler. • La coupure du câble peut affecter de nombreux utilisateurs. • Le bus est facile à étendre.
Anneau	• Accès égal pour tous les ordinateurs. • Performances régulières même si les utilisateurs sont nombreux.	• La panne d'un ordinateur peut affecter le reste du réseau. • Problème difficile à isoler. • La reconfiguration du réseau interrompt son fonctionnement.
Maillée	• Redondance, fiabilité et facilité de dépannage	• Coûteux en câblage.
Etoile	• Il est facile d'ajouter des ordinateurs et de procéder à des modifications. • Possibilité de centraliser la surveillance et l'administration. • La panne d'un ordinateur n'a pas d'incidence sur le reste du réseau.	• Si le point central tombe en panne le réseau est mis hors service.

Tableau I.1: Comparaison des différentes topologies.

I.3.2. Topologie logique

Les topologies logiques les plus fréquentes sont :

I.3.2.1.Token ring : Le terme Token ring signifie « anneau à jeton » caractérise la technique liée pour attribuer la parole. Le réseau est construit pour une technologie en anneau. Chaque station est reliée à la station précédente et à la suivante. Chaque station de l'anneau reçoit la trame de son prédécesseur et la transmet vers son successeur.

I.3.2.2.Ethernet : Dans un réseau Ethernet, la communication se fait par un protocole CSMA/CD (Carrier Sense Multiple Access /collision Detect), pour éviter toutes sortes de collision, on

utilise CSMA/CD. Il assure une très grande surveillance sur les données transmises et si une station veut émettre, elle doit s'assurer que le canal est libre. Cela revient au droit d'accès multiple. Mais si deux ou plusieurs stations tentent d'émettre au même temps, on aura une collision. Pour gérer ce problème, on utilise la technique des collisions (Collision Detect).

I.4. Architectures des réseaux informatiques [3]

C'est la représentation structurelle d'un réseau. Il existe deux types de fonctionnement :

- Poste à poste.
- Client/serveur.

I.4.1. Poste à poste

L'architecture poste à poste ou égale à égale ou peer to peer, comporte généralement une dizaine de postes. Chaque poste est libre de partager ses ressources et ses données ne sont pas centralisées.

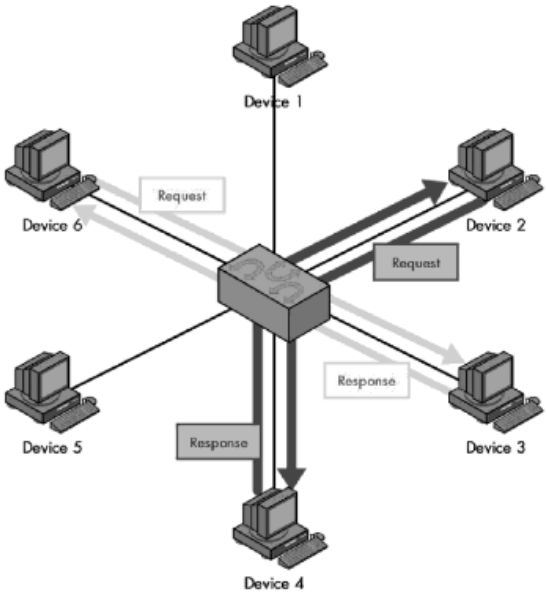

Figure I.6 : Architecture poste à poste.

I.4.2. Client /serveur

De nombreuses applications fonctionnent selon un environnement client-serveur. Cela signifie qu'il y a des stations qui sont des postes « poste client », les autres stations sont liées à une ou plusieurs taches spécialisées « serveur ».

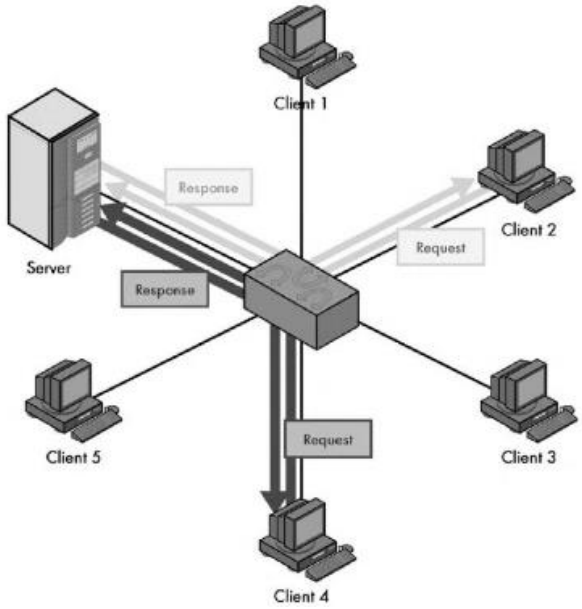

Figure I.7 : Architecture client/serveur.

I.4.3. Type d'architecture de réseau à installer : Le type d'architecture de réseau à installer dépend de ces critères :

- Taille de l'entreprise.
- Niveau de sécurité nécessaire.
- Type d'activité.
- Niveau de compétence d'administration disponible.
- Volume du trafic sur le réseau.
- Besoin des utilisateurs sur le réseau.

I.5. Normalisation [4]

La normalisation est un ensemble de règles établies qui doivent être suivies par les entités désirant communiquer. Parmi les organismes de normalisation, on trouve :

- Organisation Internationale de Normalisation (OSI).
- Union Internationale des Télécommunications-Télécommunication (UIT-T).

I.5.1. Modèle Open System Interconnexion (OSI)

Le modèle OSI est le principal modèle de réseau qui a été créé pour aider les concepteurs à mettre en œuvre des réseaux compatibles en assurant une meilleure compatibilité et interopérabilité entre les diverses technologies.

I.5.2. Couches de modèle OSI : Le modèle OSI est composé de 07 couches. Chaque couche respecte les ordres de son supérieur. Les couches de modèle OSI sont :

1) Couche physique.
2) Couche liaison de donnée.
3) Couche réseau.
4) Couche transport.
5) Couche session.
6) Couche présentation.
7) Couche application.

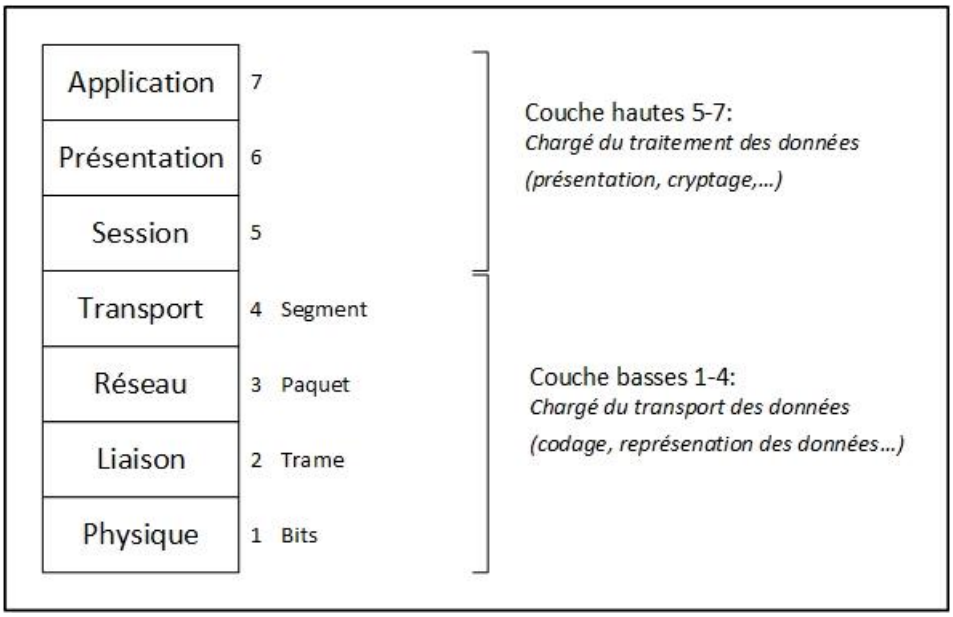

Figure I.8 : Modèle de référence OSI.

Les couches de modèle OSI sont réparties en couches :

- Couches hautes (de la couche 5 à 7), ses éléments sont purement logiciels.
- Couches intermédiaires (couches 3 et 4), comprennent des éléments logiciels et matériels.
- Couches basses (couches 1et 2), comprennent des éléments purement matériels.

I.5.2.1. Couche physique : Cette couche s'occupe des techniques de communication avec l'interface physique afin de faire transiter ou de récupérer les données sur le support de transmission.

I.5.2.2. Couche liaison de données : Cette couche s'occupe de la transmission de l'information, de la détection et la correction des erreurs. le protocole utilisé est CRC (Cyclic Redundancy Check).

I.5.2.3. Couche réseau : Le rôle de cette couche est l'adressage ainsi que le routage (sélection de meilleur chemin sur un inter-réseau).

I.5.2.4. Couche transport : Cette couche est responsable du bon acheminement des messages de l'émetteur vers le destinataire.

I.5.2.5. Couche session : Organise et synchronise les échanges et les communications.

I.5.2.6. Couche présentation : Cette couche sert à structurer et convertir les données échanges et assurer la communication entre les neouds disparates.

I.5.2.7. Couche application : Cette couche est la plus protocole de l'utilisation. Toutes les applications de communication l'utilisent sur un LAN ou sur internet.

I.5.3. Encapsulation [1]

L'encapsulation est un processus de conditionnement des données consistant à ajouter un entête de protocole déterminé avant que les données ne soient transmises à la couche inférieure.

Lorsqu'une couche N reçoit des données, elle encapsule ces dernières avec ses informations puis les passe à la couche N-1. Cette couche va construire un entête. Ce dernier et ces données vont devenir les données de la couche N-2.

Le mécanisme inverse a lieu au niveau du destinataire où une couche N+1 réceptionne les données de la couche inférieure, après, elle enlève les informations qui la concernent, puis transmet les informations restantes à la couche supérieure.

Pour identifier les données lors de leur passage au travers d'une couche, on utilise l'application Unité de Données de Protocole (PDU).

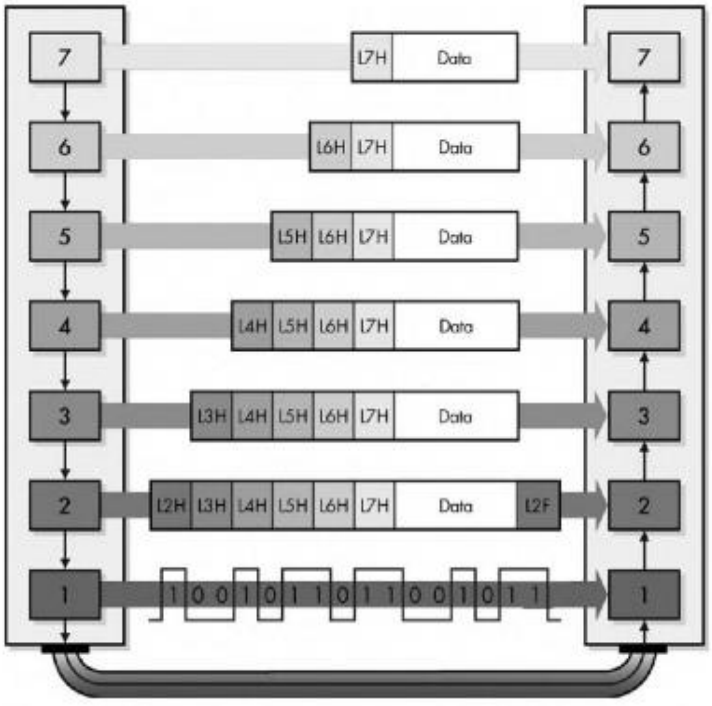

Figure I.9 : Processus d'encapsulation et décapsulation.

I.6. Modèle TCP/IP [3]

Le modèle TCP/IP (transmission contrôle protocole /Internet protocole) désigne en fait deux protocoles étroitement liés. Ce modèle est plus pratique que le modèle OSI.

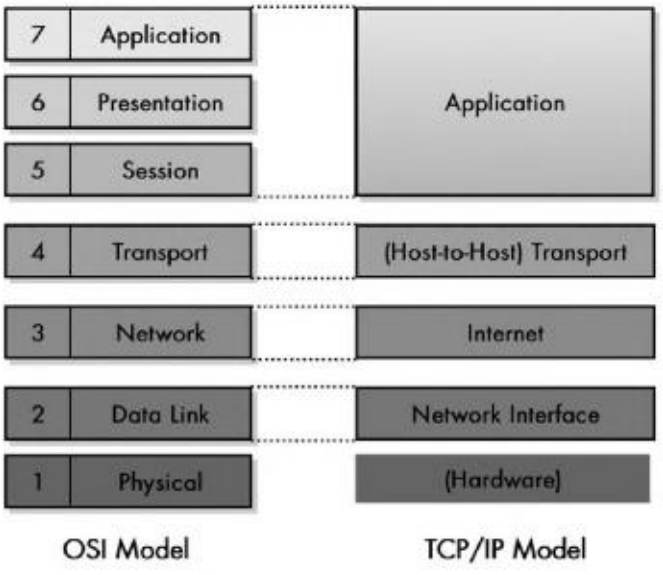

Figure I.10 : Modèle TCP/IP.

Le modèle TCP/IP peut être décrit comme une architecture réseau à 04 couches :

- Couche application (application layer).
- Couche transport (transport layer).
- Couche Internet (Internet layer).
- Couche Interface réseau (Network Access layer).

Matériel (n'est pas une couche comprise dans le protocole).

I.6.1. Couche application : Elle englobe les applications standards du réseau.

I.6.2. Couche transport : Elle assure l'acheminement des données ainsi que les mécanismes permettant de connaitre l'état de la transmission.

I.6.3. Couche Internet : Elle est chargée de fournir le paquet de données (DATA GRAMME).

I.6.4. Couche Interface réseau (Network Access layer) : Elle spécifie la forme sous laquelle les données doivent être acheminées entre émetteur et destinataire au niveau des adresses MAC.

I.7. Adressage IP [3]

De manière générale, les adresses forment une notion importante en communication et elles sont un moyen d'identification. Dans un réseau informatique, une adresse IP (Internet Protocol) est un identifiant unique attribué à chaque interface avec un réseau IP associé à une

machine (routeur, ordinateur, …). Une adresse IP est constituée de deux parties : une adresse de réseau (netid) et une adresse de machine (hostid).

I.7.1. Notion de netid et hostid : Les adresses IP sont décomposées en deux parties :

- Une partie qui identifie le réseau auquel appartient l'hôte (NET_ID).
- Une partie qui identifie le numéro de l'hôte dans le réseau (HOST_ID).

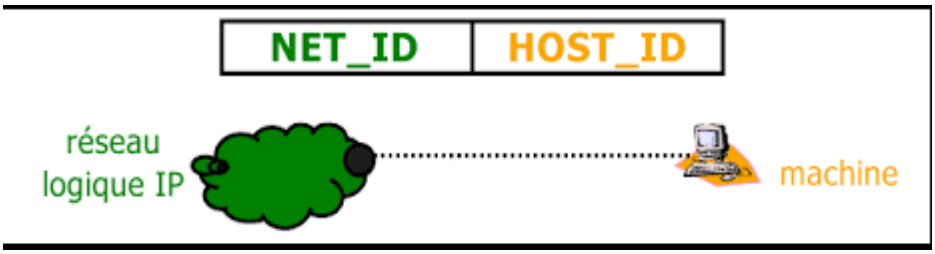

Figure I.11 : Notion de netid et hostid.

I.7.2. Différentes types des adresses IP

Il existe deux types d'adresse IP : IPv4 et IPv6.

I.7.2.1. IPv4 : Les adresses IPv4 sont codées sur 32 bits**.** Elles sont généralement notées avec quatre nombres compris entre 0 et 255, séparés par des points. C'est le plus utilisée actuellement. Il se divise en deux :

- **Les adresses privées :** Sont attribuées pour tous les administrateurs de réseau pourvu qu'elles ne soient pas routées sur Internet.
- **Les adresses publiques :** Sont délivrées par une structure mondiale qui assure l'unicité.

I.7.2.1.1. Décomposition des adresses IPv4

La décomposition d'une adresse IP se fait par un masque. Chaque équipement effectuera une opération ET (bit à bit) entre l'adresse IP et le masque. Il suffit juste de placer des bits à 1 dans le masque pour conserver le **netid** et des 0 pour écraser le **hostid**. Le masque a la même longueur qu'une adresse IP.

- Pour déterminer la partie réseau (netid) auquel appartient un équipement, l'opération suivante est réalisée :

Netid : Une opération ET bit à bit entre l'adresse IP et le masque.

Exemple : 192.168.52.0 -- 192.168.52.85 & 255.255.255.0

- Pour déterminer le numéro de l'hôte (*hostid*) dans le réseau, l'opération suivante est réalisée :

Hostid : Une opération ET bit à bit entre l'adresse IP et le masque.

Exemple : 0.0.0.85 -- 192.168.52.85 & 0.0.0.255

- Lorsque tous les bits du hostid sont à 1, on obtient une adresse de broadcast. C'est une adresse de diffusion générale pour toutes les machines du réseau (**Exemple :** 192.168.52.255 avec un masque 255.255.255.0), c'est une adresse interdite.

I.7.2.1.2. Taille d'un réseau IPv4

La taille d'un réseau IPv4 est définit par le masque, c'est-à-dire la plage d'adresses assignables aux machines du réseau. Le masque 255.255.0.0 possède 16 bits à 1 et découpe l'adresse IP de la manière suivante :

- Le netid fera donc 16 bits (valeur fixée par le masque).
- Nombre de bits restant pour le hostid : 32 - 16 = 16 bits.

I.7.2.2. IPv6 : Les adresses sont codées sur 128 bits. Elles sont généralement notées par groupes de 4 chiffres hexadécimaux séparés par '**:**'.

I.7.3. Classes d'adresses IP [3]

À l'origine, plusieurs groupes d'adresses ont été définis dans le but d'optimiser le routage des paquets entre les différents réseaux. Ces groupes ont été appelés classes d'adresses IP. Ces classes correspondent à des regroupements en réseaux de même taille. Les réseaux de la même classe ont le même nombre d'hôtes maximum. Les classes d'adresses IP sont :

- **Classe A :** Est la classe des très gros réseaux tel que ARPANET et MILNET, elle comporte 126 réseaux de 17 millions de machines chacune. Elle contient 8 bits utilisés pour l'adresse réseau et 24 bits pour l'adresse machine. Le premier bit du poids fort est à " 0 " Zéro.
- **Classe B :** Est la classe des réseaux moyens, elle comporte 16384 réseaux de 65000 machines. elle contient 16 bits utilisés pour l'adresse réseau et 16 bits pour l'adresse machines. Les deux premiers bits du poids fort sont à "10 ".
- **Classe C :** Est la classe des réseaux locaux, c'est la classe la plus utilisée dans l'Internet. Elle comporte deux millions de réseaux de 254 machines chacune. Elle contient 24 bits utilisés pour l'adressage réseaux et 8 bits pour l'adressage machines. Les trois premiers bits du poids fort sont à " 110 ".
- **Classe D :** Est la classe de diffusion multiple (Multicast). Elle contient 8 bits utilisés pour l'adressage réseaux et 24 bits pour l'adressage machines. Les quatre premiers bits du poids fort sont à " 1110 ".
- **Classe E :** Est une classe expérimentale réservée à des usages d'essais ou des usages futurs. Elle contient 8 bits utilisés pour l'adressage réseaux et 24 bits pour l'adressage machines. Les quatre premiers bits du poids fort sont tous à " 1111 ".

I.8. Equipements d'interconnexion [2]

Pour relier les périphériques informatiques on a besoin des périphériques spécialisés pour créer le réseau local. Les équipements d'interconnexion les plus utilisés sont :

I.8.1. Carte réseau

La carte réseau ou NIC (Network Interface Card) constitue l'interface physique entre l'ordinateur et le support de communication. Pour qu'un ordinateur soit mis en réseau, il doit être muni d'une carte réseau. Elle possède généralement deux témoins lumineux (LED).

- La LED verte indique l'alimentation de la carte.
- La LED orange (10Mb/s) indique une activité du réseau (envoie ou réception de données).

Figure I.12: Carte réseau.

I.8.2. Répéteur

C'est un équipement qui opère au niveau de la couche 1 du modèle OSI (Couche physique). Il a pour rôle d'étende la distance du câblage.

Figure I.13: Répéteur.

I.8.3. Concentrateur (HUB)

C'est un équipement qui opère au niveau de la couche 1 du modèle OSI. Il assure la continuité du réseau sur chacune de ses prises. Sont but est de permettre le branchement ou le débranchement des stations sans perturber le fonctionnement global du réseau.

Figure I.14 : Concentrateur (HUB).

I.8.4. Commutateur (Switch)

Un commutateur est un équipement qui relie des stations sur un même réseau local, il ne se contente pas de reproduire sur tous les ports chaque trame qu'il reçoit.

Figure I.15 : Commutateur (Switch).

I.8.5. Pont

Le pont est un équipement qui opère au niveau 2 du modèle OSI (couche liaison de données), son rôle est de relier les réseaux en filtrant les trames Les ponts permettent de diminuer la charge d'un réseau local en le déversant en deux sous réseaux.

Figure I.16 : Pont.

I.8.6. Routeur

Il opère au niveau 3 du modèle OSI (couche réseau), il prend la décision de [TCP/IP]

Figure I.17 : Routeur.

I.8.7. Modem

Le modem (modulateur /démodulateur) est un appareil qui sert à lier un ordinateur à une ligne téléphonique. Sans un modem, on ne peut pas accéder à Internet. Il utilise un câble Rj45 pour se connecté à un ordinateur et un câble RJ11 pour une ligne téléphonique.

Figure I.18 : Modem.

I.8. Passerelle

Une passerelle est un logiciel installé dans un routeur. Elle fonctionne sur toutes les couches du modèle OSI. Elle est considérée comme un convertisseur de protocole qui peut accepter et transférer des paquets dans des réseaux en utilisant un protocole différent.

I.9. Protocoles [5]

Les protocoles sont des ensembles de règles et de procédures à respecter pour émettre et recevoir des données sur un réseau.

Voici quelques protocoles les plus utilisés :

- **Protocoles TCP/IP :** Sont formalisés par l'Internet Engineering Task force (IETF) dans des documents publics nommés RFC (Requests for Comments), les RFCs ne sont pas obligatoirement des standards. Leurs buts peuvent être : informationnel, expérimental, best current pratice. L'IETF dépend de l'ISOC.

- **Protocoles LAN/ WAN /PAN :** Sont formalisés par l'IEEE (IEE 802), l'ITU et par l'ANSI (Américain National Standards Institue).

Conclusion

Dans ce chapitre, nous avons présentés des notions de bases sur les réseaux informatiques et plus précisément les réseaux LAN. Dans le chapitre suivant, nous allons aborder la présentation d'un réseau LAN.

Chapitre II :

Sécurité de réseau LAN

II. Introduction

Les communications sont vitales pour l'enseignement et la recherche. On appelle tous les moyens matériels et logiciels qui permettent à un système de fonctionner normalement et qui ne devront être accessibles que par les personnes autorisées : sécurité informatique. Elles englobent trois principaux objectifs : [06]

- **L'intégrité :** S'assurer que les données sont bien celles qu'on croit être.
- **La confidentialité :** Seule les personnes autorisées ont l'accès aux ressources.
- **La disponibilité :** Assurer le bon fonctionnement du système informatique.

II.1. Concept de sécurité informatique et réseau underlying (sous-jacente) [07]

Les tâches de la sécurité du réseau consistent à assurer la confidentialité, l'intégrité, la non-répudiation, l'authenticité et la disponibilité des données utiles qui sont transmises dans les réseaux publics ou stockées dans des ordinateurs en réseau.

II.1.1. Confidentialité

Préserver les restrictions autorisées sur l'accès et la divulgation des informations y compris les moyens de protéger la vie privée et les informations exclusives. Une perte de confidentialité est la divulgation non autorisée d'informations.

Les termes vie privée et secret sont parfois utilisés pour distinguer la protection des données personnelles (vie privée) et la protection des données appartenant à une organisation (secret). En examinant les problèmes de confidentialité, vous serez également confronté à la question de savoir si vous souhaitez uniquement masquer le contenu d'un document à une vue non autorisée ou également son existence. Vous devez tenir compte de la confidentialité des données à la fois lorsqu'elles sont stockées sur un ordinateur et lorsqu'elles sont transmises sur le réseau. Une autre considération est de garantir la confidentialité des données stockées sur des ordinateurs portables ou des périphériques amovibles tels qu'une clé USB (Universal Serial Bus). Il y a eu plusieurs incidents récents impliquant des ordinateurs portables manquants qui stockent des données confidentielles.

II.1.2. Intégrité

Il est assez difficile de donner une définition concise de l'intégrité. En général, l'intégrité consiste à s'assurer que tout est tel qu'il est censé être et, dans le contexte de la sécurité informatique, à empêcher la modification non autorisée des informations.

D'un point de vue systématique, l'intégrité est mieux définie en fonction de l'état du système. L'Orange Book (ou Trusted Computer System Evaluation Criteria, développé par le Département de la Défense des États-Unis) définit l'intégrité de cette manière : comme l'état qui existe lorsque les données informatisées sont les mêmes que celles des documents sources et qui n'ont pas été exposées, à une altération ou à une destruction accidentelle ou malveillante.

L'intégrité est également un problème lorsque les données sont transmises sur un réseau. Un attaquant pourrait intercepter et modifier des paquets de données sur le réseau si l'intégrité de ces données n'est pas protégée. Ce type d'attaque est connu sous le nom d'attaque de l'homme du milieu.

II.1.3. Disponibilité

Dans le contexte de la sécurité, nous voulons nous assurer qu'un attaquant malveillant ne peut pas empêcher les utilisateurs légitimes d'avoir un accès raisonnable à leurs systèmes. C'est-à-dire que nous voulons empêcher le déni de service.

L'une des premières attaques par déni de service, une attaque schtroumpf est expliquée ci-dessous. Une attaque de schtroumpf oblige l'attaquant à usurper (faire semblant d'être quelqu'un que vous n'êtes pas) l'identité de la victime.

Dans une attaque schtroumpf, l'attaquant envoie une requête d'écho ICMP (Internet Control Messaging Protocol) à l'adresse de diffusion d'un réseau avec une adresse d'expéditeur usurpée (l'adresse de la victime). La demande d'écho sera distribuée à tous les nœuds de ce réseau. Chaque nœud répondra à l'adresse de l'expéditeur falsifié, inondant la victime de paquets de réponse d'écho (echo reply).

II.1.4. Authenticité

L'authenticité est l'assurance qu'un message, une transaction ou un autre échange d'informations provient de la source dont il prétend provenir. L'authenticité implique une preuve d'identité.

Nous pouvons vérifier l'authenticité grâce à l'authentification. Le processus d'authentification implique généralement plus d'une « preuve » d'identité (bien qu'une seule puisse être suffisante). La preuve peut être quelque chose qu'un utilisateur connaît, comme un mot de passe. Où un utilisateur peut prouver son identité avec quelque chose qu'il possède comme une carte-clé. Les méthodes d'authentification biométrique incluent des éléments tels que les analyses d'empreintes digitales, les analyses de la géométrie de la main ou les analyses de la rétine.

II.1.5. Non-répudiation

La non-répudiation fournit une preuve indéniable qu'une action spécifique a eu lieu. Les services de non-répudiation typiques de la sécurité des communications sont la non-répudiation de l'origine fournissant des preuves sur l'expéditeur d'un document et la non-répudiation de la remise, fournissant des preuves du fait qu'un message a été remis à un destinataire spécifique.

Un exemple physique de non-répudiation est l'envoi d'une lettre avec accusé de réception demandé. Lorsque vous le faites, une personne doit signer pour la lettre. Ceci est un exemple de non-répudiation de livraison car vous pouvez prouver que la lettre a été livrée.

Bien sûr, la personne qui signe la lettre peut ne pas être la personne à qui la lettre était adressée. Cela soulève une faiblesse potentielle dans la non-répudiation.

Supposons que la personne qui signe la lettre falsifie le nom du destinataire. Cela signifie que la livraison peut être répudiée (refusée) par le destinataire réel.

II.2. Types des attaques de ce jour [08]

Il existe plusieurs attaques informatiques, voici les plus courantes :

II.2.1. Attaques DDOS (Distributed Denial of Service) ou attaques par déni de service

Sont faites pour submerger les ressources d'un système pour qu'il ne puisse plus répondre aux demandes et elles peuvent aussi lancer un autre type d'attaques.

II.2.2. Man-in-the-Middle attaque (MitM)

Son Principe et de s'insérer dans les communications entre un serveur et un client, il y'a plusieurs :

- **Détournement de session :** L'attaque détourne entre un client de confiance et un serveur réseau. Elle cible l'adresse IP du client pendant que le serveur poursuit la session, croyant qu'il s'agit du client.
- **Usurpation d'IP :** Dans cette attaque le Hacker utilise une adresse IP volée pour assurer au système qu'il est un client fiable et connu.
- **Replay :** L'attaquant intercepte et enregistre les anciens messages et tente plus tard de les envoyer se faisant passer pour quelqu'un de confiance.

II.2.3. Drive-by download ou téléchargement furtif

C'est une méthode de propagation des logiciels malveillants. Il insère un virus sur une page d'un site non sécurisé et infecte les ordinateurs de ceux qui le visent qui ont des failles de sécurité par exemple des mises à jour non installées.

II.2.4. Attaques par mot de passe

Pour trouver un mot de passe il faut surveiller la connexion d'un bureau et trouver un mot de passe non chiffré en ayant recours à l'ingénierie sociale ou en devinant :

- **Par force brute :** Deviner ce que les gens ont fait comme mot de passe, nom, prénom, date de naissance, …..etc.
- **Par dictionnaire :** Copier un fichier chiffré contenant des mots de passe courants et comparer les résultats.

II.2.5. Injection SQL (Structured Query Language)

Cette attaque passe par trois étapes : l'exécution, l'insertion et l'exploitation. Au début le Hacker exécute une requête SQL sur la base de données via les données

entrantes du client vers le serveur, puis il insère les commandes SQL dans une entrée du plan de données et il peut mettre à jour ou supprimer les données et envoyer même des commandes au système d'exploitation.

II.2.6. Logiciels malveillants ou malwares

Sont des logiciels indésirables installés dans nos systèmes sans notre acceptation, voici quelques –uns :

- **Chevaux de trois :** Ils se cachent dans un programme utile pour ensuite se déployer.
- **Vers :** Sont des programmes autonomes qui se propagent sur les réseaux et les ordinateurs.
- **Ransomwares :** C'est un type de logiciel malveillant qui crypte les données d'un ordinateur et exige une rançon à la victime contre son déchiffrement.

II.2.7. Intrusions sur les objets connectés

Ces intrusion son plus utilisées sur les objets connectés facilement piratables.

II.2.8. Attaques Géopolitiques

Sont des attaques faites par certains pays contre d'autres pour voler certaines technologies dans un cadre d'espionnage industriel ou pour les déstabiliser.

II.2.9. Gross –site Scripting (XSS)

Dans cette opération le Hacker injecte le contenu dans une page qui corrompt le navigateur de la cible, ensuite il peut modifier la page web selon son but ; il peut voler des informations sur les cookies, récupérer des données sensibles pour contrôler à distance l'ordinateur de sa victime.

II.2.10. Attaques de phishing

C'est la fenêtre la plus connue qui surgit en vous disant que vous avez gagné une voiture. Cette technologie réunit entre ingénierie sociale et stratagème technique, vous pousse à télécharger par vous-même des malwares pour voler vos informations personnelles et confidentielles.

II.2.11. Attaques cyber physiques

Ces attaques visent les systèmes de transport, d'usines, réseaux électriques, etc.

II.2.12. Attaques contre les appareils et dossiers médicaux

Il y a de nombreuses technologies et aussi des données très confidentielles. Nous voyons qu'elles sont dangereuses si elles pouvaient avoir accès aux appareils médicaux par les cybercriminels.

II.3. Difficultés de se défendre contre les attaques [09]

Le défi de sécuriser les ordinateurs n'a jamais été aussi grand, non seulement en raison du nombre d'attaques mais aussi en raison des difficultés rencontrées pour se défendre contre ces attaques. Ces difficultés sont les suivantes :

- **Appareils connectés de manière universelle :** C'est impensable aujourd'hui pour n'importe quel appareil technologique, Ordinateur de bureau, tablette, ordinateur portable ou Smartphone ne pas être connecté à Internet. Bien que cela offre d'énormes avantages, cela facilite également la tâche d'un attaquant à l'autre bout du monde pour lancer silencieusement une attaque contre un appareil connecté.
- **Augmentation de la vitesse des attaques avec des outils modernes à leur disposition :** Les attaquants peuvent rapidement scanner des millions d'appareils pour trouver des faiblesses et lancer des attaques. La plupart des outils d'attaque lancent de nouvelles attaques sans aucune participation humaine.
- **Une plus grande sophistication des attaques :** Les attaques deviennent plus complexes, ce qui rend plus difficile à détecter et à se défendre contre elles. Les attaquants utilisent aujourd'hui des protocoles Internet et applications pour effectuer des attaques, ce qui rend plus difficile à distinguer une attaque du trafic légitime. D'autres outils d'attaque varient leur comportement afin que la même attaque apparaisse différemment à chaque fois. Ceci complique d'avantage leurs détections.
- **Disponibilité et simplicité des outils d'attaque :** Dans le passé, un attaquant devait avoir une connaissance technique approfondie des réseaux et des ordinateurs ainsi que la capacité d'écrire un programme pour générer l'attaque, ce n'est plus le cas. Les outils d'attaque logicielle d'aujourd'hui ne nécessitent pas de connaissances sophistiquées de la part de l'attaquant. En fait, de nombreux outils ont une interface

utilisateur graphique (GUI) qui permet à l'utilisateur de sélectionner facilement des options dans un menu. Ces outils sont disponibles gratuitement ou peuvent être achetés auprès d'autres attaquants à un coût étonnamment bas.

- **Détection plus rapide des vulnérabilités :** La faiblesse du matériel et des logiciels peut être plus rapidement découverte et exploitée avec de nouveaux outils logiciels et techniques.
- **Retards dans la mise à jour de sécurité :** Les fournisseurs de matériel et de logiciels sont débordés d'essayer de suivre le rythme de la mise à jour de leurs produits contre les attaques. Le logiciel antivirus de l'institut de sécurité reçoit plus de 200 000 soumissions de logiciels malveillants potentiels chaque jour. À ce rythme, les éditeurs d'antivirus devraient créer et distribuer des mises à jour toutes les quelques secondes pour garder les utilisateurs entièrement protégés. Ce retard dans la diffusion des mises à jour de sécurité s'ajoute aux difficultés de défense contre les attaques, par une mauvaise distribution des mises à jour de sécurité, malgré que les fournisseurs de produits de consommation tels que Microsoft, Apple et Adobe disposent d'un système pour informer les utilisateurs des mises à jour de sécurité. De plus, ces fournisseurs ne créent souvent pas de petites mises à jour de sécurité qui « corrigent » le logiciel existant, au lieu de cela, elles résolvent le problème dans une toute nouvelle version du logiciel et demandent ensuite à l'utilisateur de payer pour une nouvelle version qui contient le correctif. Les attaquants d'aujourd'hui se concentrent davantage pour découvrir et exploiter les vulnérabilités de ces produits.
- **Attaques distribuées :** Les attaquants peuvent utiliser des centaines de milliers d'ordinateurs sous leur contrôle dans une attaque contre un seul serveur ou réseau. Ce « plusieurs contre un » rend pratiquement impossible l'arrêt d'une attaque en identifiant et en bloquant une source unique.
- **Présentation du BYOD (Bring Your Own Device) :** Il y a peu, les services informatiques étaient «autocratiques» : ils établissent des normes technologiques pour les utilisateurs en leur spécifiant quels appareils pourraient être achetés en refusant d'autoriser des appareils personnels à connecter aux réseaux de l'entreprise. Cependant, coïncidant avec l'introduction des ordinateurs tablettes modernes en 2010 et l'utilisation généralisée de Smartphones, les utilisateurs ont commencé à faire pression sur les services informatiques pour leur permettre d'utiliser et connecter leurs appareils personnels au réseau de l'entreprise (appelé BYOD ou apporter votre propre

appareil). Cette tendance à permettre aux employés d'utiliser leurs propres appareils personnels pour se connecter au réseau de l'entreprise a rendu difficile pour les services informatiques de fournir une sécurité adéquate pour une gamme presque infinie d'appareils qu'ils ne possèdent pas. Les utilisateurs sont de plus en plus appelés à prendre des décisions de sécurité difficiles concernant leurs systèmes informatiques parfois avec peu ou pas d'informations pour les guider. Il n'est pas rare qu'un utilisateur se voit poser des questions de sécurité telles que : Voulez-vous afficher uniquement le contenu qui a été livré en toute sécurité ? Ou est-il sûr de mettre en quarantaine cette pièce jointe ? Ou voulez-vous installer ce module complémentaire ? Avec peu ou pas de direction, les utilisateurs sont enclins à fournir des réponses aux questions sans comprendre les risques de sécurité, et cela résume les raisons pour lesquelles il est difficile de se défendre contre les attaques d'aujourd'hui.

II.4. Mécanismes de sécurité [10]

La sécurité des réseaux repose généralement sur la restriction ou le blocage d'opérations à partir de systèmes distants et pour assurer la sécurité de ces systèmes, on utilise des mécanismes qui évitent les intrusions. Voici certains de ces mécanismes :

- **Chiffrement :** Algorithme généralement basé sur des clefs et transformant les données. Sa sécurité est dépendante du niveau de sécurité des clefs.
- **Signature numérique :** Données ajoutées pour vérifier l'intégrité ou l'origine des données.
- **Bourrage de trafic :** Données ajoutées pour assurer la confidentialité, notamment au niveau du volume du trafic.
- **Notarisation :** Utilisation d'un tiers de confiance pour assurer certains services de sécurité.
- **Contrôle d'accès :** Vérifie les droits d'accès d'un acteur aux données. N'empêche pas l'exploitation d'une vulnérabilité.
- **Antivirus :** Logiciel censé protéger l'ordinateur contre les logiciels (ou fichiers potentiellement exécutables) néfastes. Ne protège pas contre un intrus qui emploie un logiciel légitime ou contre un utilisateur légitime qui accède à une ressource alors qu'il n'est pas autorisé à le faire.

- **Pare-feu :** Un élément (logiciel ou matériel) du réseau informatique contrôlant les communications qui le traversent. Il a pour fonction de faire respecter la politique de sécurité du réseau qui définit quels sont les communications autorisées ou interdites. Il n'empêche pas un attaquant d'utiliser une connexion autorisée pour attaquer le système et ne protège pas contre une attaque venant du réseau intérieur (qui ne le traverse pas).
- **Détection d'intrusion :** Repère les activités anormales ou suspectes sur le réseau surveillé. Ne détecte pas les accès incorrects mais autorisés par un utilisateur légitime. Mauvaise détection : taux de faux positifs, faux négatifs.
- **Journalisation (logs) :** Enregistrement des activités de chaque acteur, permet de constater que des attaques ont eu lieu, de les analyser et potentiellement de faire en sorte qu'elles ne se reproduisent pas.
- **Analyse des vulnérabilités (security audit) :** Identification des points de vulnérabilité du système. Ne détecte pas les attaques ayant déjà eu lieu ou lorsqu'elles auront lieu.
- **Contrôle du routage :** Sécurisation des chemins (liens et équipements d'interconnexion).
- **Contrôle d'accès aux communications :** Le moyen de communication n'est utilisé que par des acteurs autorisés par VPN (Virtual Private Network) ou tunnels.
- **Horodatage :** Marquage sécurisé des instants significatifs.
- **Certification :** Preuve d'un fait, d'un droit accordé.
- **Distribution de clefs :** Distribution sécurisée des clefs entre les entités concernées.
- **Authentification :** Authentifier les utilisateurs, c'est–à-dire de leur demander de s'identifier à l'aide d'un nom d'utilisateur et d'un mot de passe par exemple : dans le domaine des communications, on authentifie l'émetteur du message. Si on considère les extrémités d'une communication il faut effectuer une double authentification. Par exemple lutter contre le "phishing", et dans l'authentification est nécessaire au bon fonctionnement des autres mécanismes.
- **La protection physique :** Peut fournir une protection totale, mais qui peut être excessive. Il peut s'agir par exemple d'isoler complètement son système.

II.5. Outils de protection d'un réseau LAN

Quand on parle de la sécurité informatique, on dit antivirus ou pare-feu (Firewall en anglais).

II.5.1. Antivirus [11]

Un antivirus est un logiciel conçu pour identifier, neutraliser et éliminer des logiciels malveillants. Il existe des antivirus gratuits comme AVAST, et payant comme NORTON, KASPERSKY.

II.5.2. Détecteurs des anomalies [12]

Il peut être difficile d'identifier les anomalies de votre réseau sans comprendre la manière dont ce réseau devrait fonctionner. Les moteurs de détection d'anomalie réseau (Network anomaly Detection Engines) (ADE) vous permettent d'analyser votre réseau, de sorte que, lorsque des violations se produisent, vous les saurez assez rapidement pour pouvoir répondre.

II.5.3. Pare-feu (Firewall) [13]

C'est le meilleur outil de protection de notre ordinateur contre les malwares. Aussi, il est efficace pour protéger les appareils qui partagent la même connexion.

Le Firewall est un logiciel ou micro logiciel qui filtre le trafic et amenuise les risques causés par les logiciels malveillants. Pour mieux le définir, nous allons essayer d'approfondir dans son propos et expliquer son concept.

II.5.3.1. Fonctionnement d'un pare-feu [14]

Le but de Firewall est de contrôler le flux d'informations qui circule entre l'ordinateur, notre réseau et l'Internet.

II.5.3.2. Avantages d'un Firewall [15]

- Pour protéger le réseau dans sa totalité, le Firewall concentre la sécurité réseau en un seul point.
- Il est impératif que l'administrateur réseau évalue régulièrement le trafic pour s'assurer qu'il n'a pas contourné ou cracké.
- Le réseau local continuera à fonctionner parce que la panne est à un seul point.

II.5.3.3. Inconvénients d'un Firewall [15]

- Il ne protège que les attaques qui passent par lui.
- Il suffit de se transformer dans un autre format lorsque le pare-feu bloque tous les fichiers de sortie.

II.6. Comparaison entre le pare-feu classique et le pare-feu de nouvelle génération [16]

II.6.1. Firewall classique

II.6.1.1. Circuit level firewall: Transport Layer

Lorsqu'un ordinateur protégé démarre une conversation avec un ordinateur distant, le trafic est intercepté par le pare-feu au niveau du circuit qui transmet la demande. Lorsque le trafic de retour atteint le pare-feu, les tables internes sont vérifiées pour établir s'il doit être transféré vers un ordinateur protégé ou s'il s'agit d'une conversation non demandée.

Le principal avantage de ce type de pare-feu est que seul le trafic de retour des conversations initiées derrière le pare-feu sera autorisé. Comme il n'y a pas de connectivité directe entre l'ordinateur protégé et le réseau externe, toutes les conversations non reconnues sont abandonnées. Cependant, cela peut également être un inconvénient car tout ce qui est demandé par l'ordinateur protégé sera reçu même s'il s'agit de contenu malveillant. Les routeurs SOHO (Small Office/ Home Office), couramment utilisés pour les connexions haut débit à domicile, fournissent généralement un pare-feu au niveau du circuit via NAT et/ou PAT.

II.6.1.2. Packet filtering Firewall: Network Layer

Les pare-feu agissant au niveau de la couche réseau ont été les premiers à être développés et sont probablement les mieux compris par les administrateurs réseau. Ils fonctionnent en examinant chaque paquet par rapport à un ensemble de règles définies. Ces règles concernent généralement :

- Adresses IP source et destination.
- Ports source et destination.
- Protocole au niveau de la couche transport ou réseau (IP, TCP, UDP, ICMP,..).
- Interface physique.
- Direction (entrée ou sortie).
- État du paquet.

Dans l'ensemble, les filtres de paquets peuvent uniquement autoriser ou supprimer et enregistrer le trafic. Le contenu du trafic n'est pas modifié. Lorsqu'un paquet est reçu, il est évalué par rapport à un ensemble de règles et une fois que le

paquet correspond à une règle, l'action définie est entreprise. Cela signifie que l'ordre des règles est critique car la première correspondance trouvée détermine ce qui arrive à ce paquet particulier. Les règles sont facilement définies à l'aide d'une logique simple. Par exemple, pour bloquer tout le trafic SMTP entrant, une règle peut être définie pour tout le trafic source TCP vers le réseau de destination local correspondant au port SMTP 25. Le filtrage de paquets peut également supprimer d'autres trafics réseau.

II.6.2. Firewall moderne

II.6.2.1. Application Firewall : Application Layer

Les pare-feux agissant au niveau de la couche application inspectent le trafic à un niveau beaucoup plus élevé que les pare-feux traditionnels. Il peut s'agir de périphériques réseau placés en ligne, de serveurs proxy pour gérer un trafic spécifique ou d'applications exécutées sur un serveur pour filtrer le trafic vers un programme particulier.

Les pare-feux de la couche application fonctionnent différemment de ceux de la couche réseau en raison de la façon dont les données sont transmises sur les réseaux. Chaque bloc de données se compose de deux parties, « l'en-tête » et la « charge utile ». (En utilisant une analogie postale, l'en-tête est l'enveloppe et la charge utile est la lettre à l'intérieur). Les conversations entre ordinateurs comprennent bon nombre de ces morceaux de données, appelés paquets. Un pare-feu de couche d'application peut inspecter la charge utile ainsi que l'en-tête et peut examiner une série de paquets ensemble.

L'une des principales caractéristiques d'un pare-feu de couche application est sa capacité à bloquer tous les paquets qui ne sont pas conformes à la norme RFC (Requests for Comments) pour le protocole inspecté. Il peut également agir comme un filtre de contenu en examinant la charge utile, les paquets contenant Java ou des logiciels malveillants peuvent être bloqués. Le contenu peut même être réassemblé et vérifié contre les virus avant d'être transmis à l'utilisateur final.

II.6.2.2. DPI Firewall (Deep Packet Inspection)

L'inspection DPI de couche 7 et d'autres termes similaires font référence au niveau auquel un pare-feu, ou même tout périphérique réseau, examine les paquets.

La technologie utilisée par les pare-feux DPI est la même que dans les pare-feux applicatifs et les deux sont souvent combinées dans les pare-feux modernes. Les paquets de l’""en-tête" et de la "charge utile" seront inspectés.

Un pare-feu DPI utilisera un ensemble de signatures plus proches d'un IDS ou d'un IPS (index de pression systolique). Lorsqu'un paquet est comparé à une signature, il peut être abandonné, étiqueté, limité en débit et enregistré. Les signatures de paquets peuvent être de simples requêtes HTTP avec cmd.exe dans l'URL ou des indicateurs plus complexes de l'activité du ver NetBIOS/SMB.

Les systèmes DPI ont une surcharge considérable. C'est pourquoi les fabricants commencent à implémenter leur code dans des ASIC (application-specific integrated circuit) en silicium pour obtenir des performances de vitesses filaires plus rapides. Cela permet à l'appareil de conserver la table d'état du pare-feu avec état ainsi que l'état actuel de l'application utilisant la conversation.

Placer la technologie de détection sur le pare-feu permet aux paquets malveillants d'être détectés et supprimés plus tôt dans leur entrée sur le réseau. Traditionnellement, un système IDS serait en mesure d'alerter l'administrateur réseau d'une telle activité où un système IPS utiliserait l'extinction de la source enverrait des réinitialisations. Rapprocher cette technologie du réseau malveillant ne peut qu'améliorer la sécurité d'une organisation.

II.7. Mode déploiement de firewall

II.7.1. Passive firewall [17]

En mode Pare-feu passif, un pare-feu de couche 2 inspecte mais ne filtre pas activement le trafic. Il peut être déployé en mode pare-feu passif de deux manières :

- En mode capture pour inspecter les paquets qui ont été dupliqués pour inspection via les ports SPAN ou miroir.
- En mode passif en ligne en configurant la machine pour n’enregistrer que les connexions par défaut.

II.7.1.1. Span mode

Dans une installation en mode capture, les paquets sont dupliqués pour inspection via un port SPAN ou miroir sur un commutateur/routeur. Dans un cluster de pare-feu de couche 2, chaque nœud doit être connecté à son propre port SPAN ou miroir.

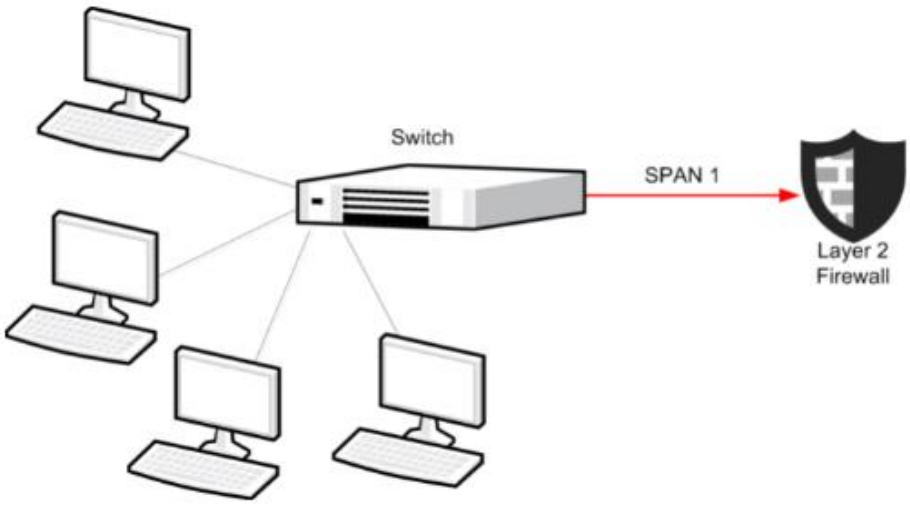

Figure II.1: Pare-feu à couche unique 2 en mode capture avec des ports SPAN/miroir.

II.7.1.2. Inline mode

Lorsque vous sélectionnez le mode de connexion du journal uniquement pour la terminaison de connexion par défaut global, vous pouvez déployer des pare-feux de couche 2 en mode de pare-feu passif dans une configuration en ligne.

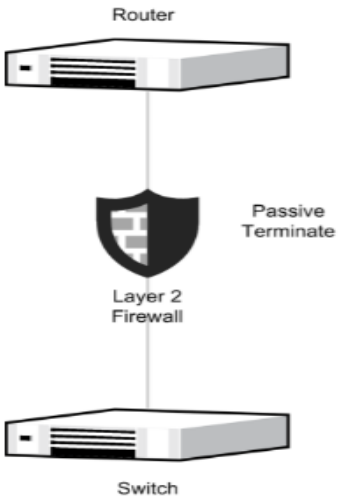

Figure II.2 : Pare-feu à couche unique 2 en mode passif en ligne.

II.7.2. Routed firewall mode [18]

En mode routed, l'appliance de sécurité est considérée comme un saut de routeur dans le réseau. Il peut effectuer un NAT (Traduction d'Adresse Réseau) entre les réseaux connectés et peut utiliser OSPF ou RIP (Routing Information Protocol). Le mode routé prend en charge de nombreuses interfaces. Chaque interface se trouve sur un sous-réseau différent. Vous pouvez partager des interfaces entre les contextes.

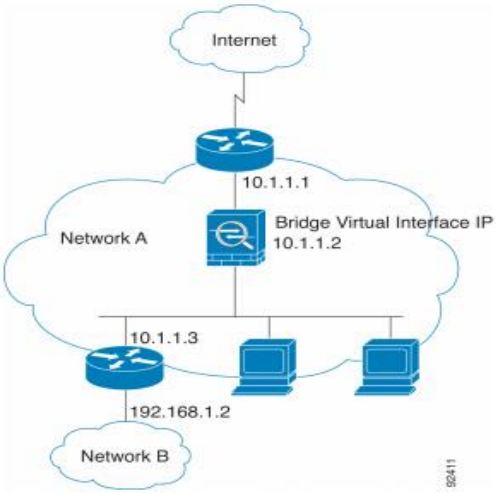

Figure II.3: Routed firewall network.

Conclusion

Dans ce chapitre, nous avons présenté la sécurité de réseau LAN, plus précisément son concept de sécurité, types des attaques avec les difficultés de se défendre contre ces derniers, mécanisme de sécurité, les outils de protection, firewall dans le passé et dans nos jours avec ces différents types. Dans le prochain chapitre, nous allons aborder notre application qui sera intitulée sur le déploiement d'un réseau LAN protégé par une Firewall d'une marque leader dans le marché Fortinet.

Chapitre III :

Déploiement d'un réseau LAN protégé par FortiGate

III . Introduction

FortiGate est un équipement de sécurité de réseau. Il est optimisé pour les segmentations internes, le Cloud, le data center, la distribution et le déploiement dans les entreprises de différentes tailles. Il simplifie notre sécurité avec une solution physique, virtuel et Cloud.

Notre travail s'est déroulé dans un site connecté à internet via une liaison satellitaire (système VSAT).

Au début de notre travail nous avons utilisé une plate forme virtuelle Emulated Virtuel Envirement- Next Generation (EVE-NG) où nous avons configuré les équipements et déployé la solution et à la fin, nous avons testé et visualisé les résultats.

III.1. Généralité sur les systèmes VSAT [19]

Le système VSAT (Very Small Aperture Terminal) est basé sur l'utilisation des satellites géostationnaires en tant que relais hertziens et cela pour émettre et recevoir des données à partir d'un terminal (HUB) de dimensions variées. Il réalise une liaison directe entre une station cliente et le système central, comme il permet aux entreprises d'interconnecter leurs sites distants au site principal afin de garantir le transfert des services, notamment les données, visioconférence, Internet et la téléphonie.

III.2. Architecture générale d'un réseau VSAT [20]

Un système de communication par satellite se compose d'un ensemble de stations terrestres qui communique ensemble via un satellite placé autour de la terre.

Une liaison satellitaire est composée de la transmission d'un signal depuis une station émettrice vers un satellite récepteur, l'amplifie et ensuite le retransmet vers une station réceptrice.

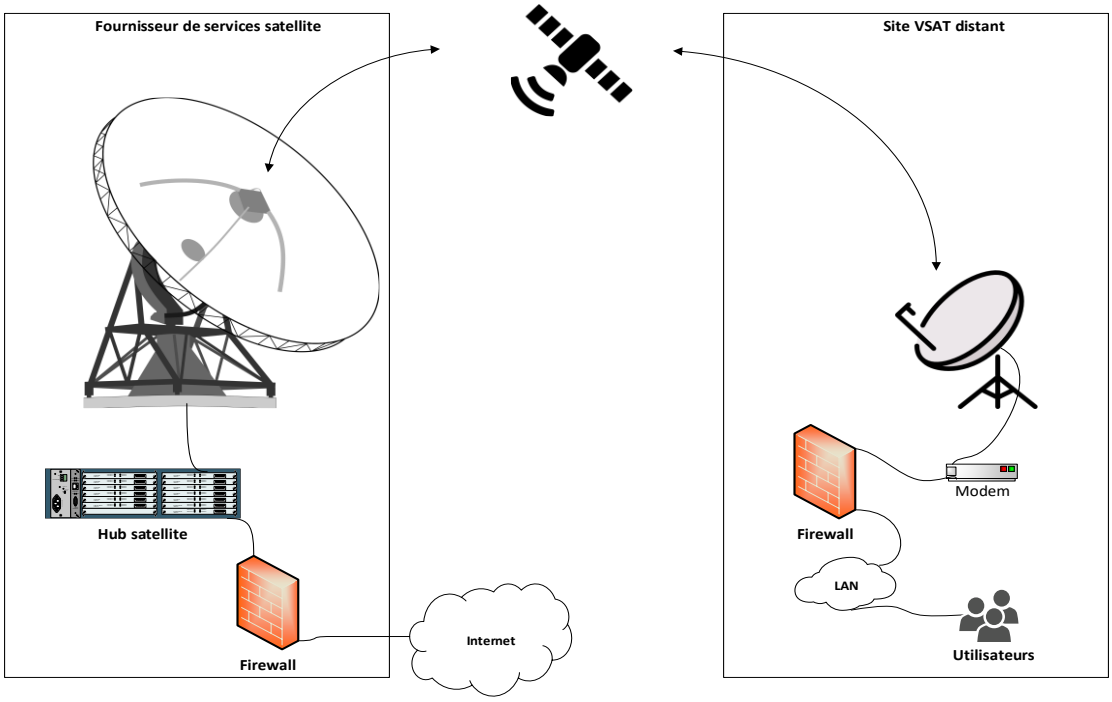

Figure III.1 : Architecture d'un réseau VSAT.

III.3. Pare-feu nouvelle génération (NGFW) FortiGate [21]

Les pare-feux NGFW FortiGate sont optimisés par des processeurs orientés sécurité SPU (Security Processing Unit), et notamment le processeur NP7 (Network Processor 7). L'approche d'un réseau orienté sécurité devient ainsi possible avec ces pare-feux adaptés aux data centers hybrides et hyperscales.

FortiGate est un levier de maîtrise des coûts et de simplification. Ces pare-feux sont une alternative au déploiement de plusieurs outils autonomes, consolidés, au sein d'une seule plateforme, différentes fonctions de sécurité (inspection SSL, filtrage Web ou encore prévention d'intrusion) pour une visibilité meilleure et protéger tous les edge réseau. Ces pare-feux sont adaptés aux besoins de performance des architectures hyperscales et hybrides, aidant ainsi les entreprises à optimiser l'expérience utilisateur, mais aussi, à assurer leur continuité métier grâce à une gestion intelligente des risques.

Les pare-feux de nouvelle génération FortiGate inspectent le trafic réseau entrant et sortant à très grande échelle. Ces inspections, rapides et évolutives, n'autorisent que le trafic légitime, sans dégradation de l'expérience utilisateur ni indisponibilité coûteuse.

En tant que partie intégrante de tissu de sécurité de Fortinet, FortiGate communique avec toutes les autres solutions Fortinet ainsi qu'avec des solutions au sein d'un environnement hétérogène. FortiGate s'intègre en toute transparence avec les services FortiGuard et avec FortiSandbox pour une protection contre les menaces connues. La productivité opérationnelle est également améliorée grâce à une intégration avec Fabric Management Center.

III.3.1. Modèle et spécification de FortiGate NGFW

Le pare-feu NGFW FortiGate se décline en différents modèles adaptés à vos besoins, d'appliance matérielles d'entrée de gamme aux appliances ultra haut de gamme qui offrent des performances maximales de protection contre les menaces. FortiGate assure ainsi la sécurité des sites d'entreprises, des data centers et des segments du réseau.

III.3.2. Cas d'utilisation de FortiGate NGFW

FortiGate NGFW accompagne la transformation digitale des entreprises en protégeant tous les edge réseau et les applications. Par le renforcement de l'efficacité opérationnelle, l'automatisation des flux de travail et garantir un haut niveau de sécurité et de protection contre les menaces. Les pare-feux NGFW FortiGate offrent une évaluation des calculs de sécurité plus élevée parmi ses concurrents ainsi que les avantages suivants :

- Gestion des risques externes de sécurité.
- Gestion des risques internes de sécurité.
- Gestion des vulnérabilités.
- Une sécurité à l'échelle hyperscale.
- Sécuriser les HUB on-ramp ver le Cloud.

III.3.3. Fonctionnalités et avantages

- **Visibilité intégrale :** L'inspection des flux chiffrés sous SSL, et TLS1.3 notamment, supprime les zones d'ombre.
- **Protection contre les menaces :** La sécurité la plus intégrée du marché avec une protection automatisée contre les menaces.
- **Intégration avec la security fabric :** Assure le partage des informations sur les menaces sur l'ensemble de la surface d'attaque pour accélérer et automatiser la protection.

- **Efficacité éprouvée de la sécurité :** Une veille sur les menaces permanente et certifiée protège contre les menaces connues et inconnues.
- **Fabric management center :** Automatisation, orchestration et traitement analytique à partir d'une console de gestion unifiée.

III.4. Emulated virtual envirement – Next Generation (EVE-NG) [22]

Nous avons déployées notre solution sur la plate forme EVE-NG. Cette dernière permet aux entreprises, fournisseurs/centres d'apprentissage en ligne, individus et aux collaborateurs de groupe de créer des preuves virtuelles de concepts, de solutions et d'environnements de formation.

III.5. Architecture générale de la station

Cette figure représente l'architecture de la solution que nous avons déployée.

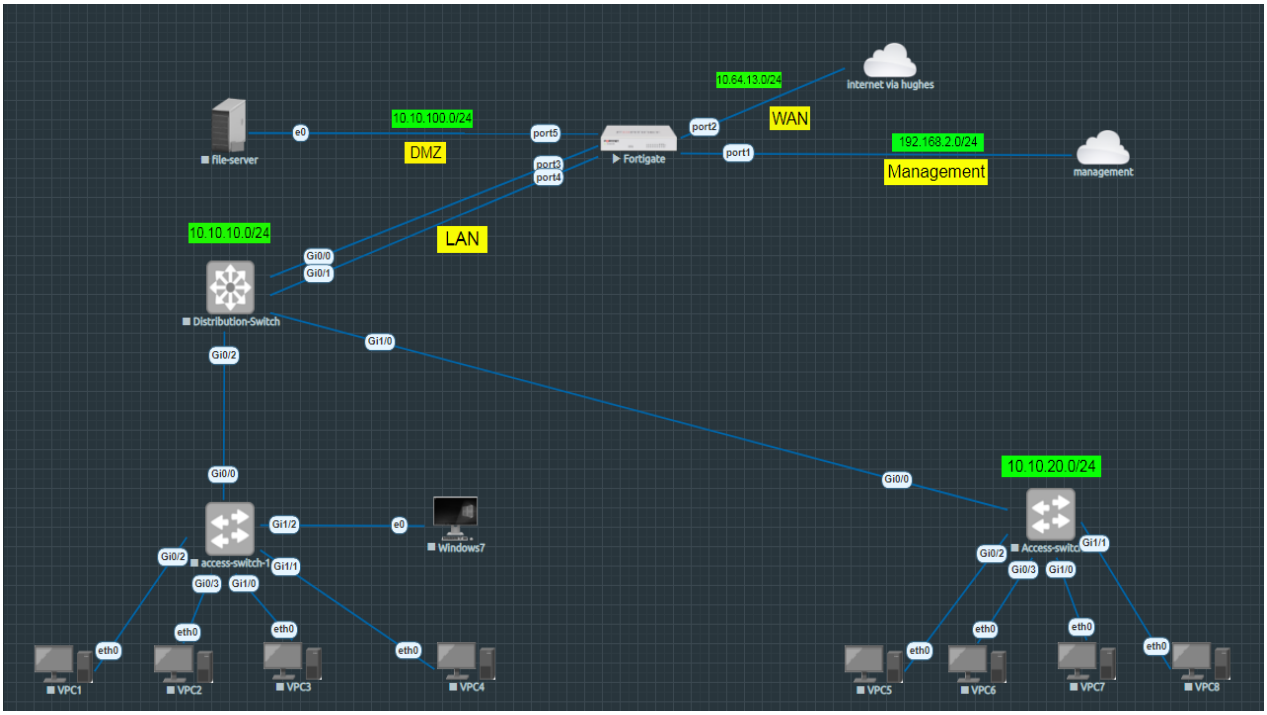

Figure III.2 : Architecture générale de la station.

III.5.1. Architecture réseau 2 tiers

Le déploiement de notre solution est caractérisé par l'architecture 2 tiers composée par un switch distribution et 2 switch access, un pour chaque département.

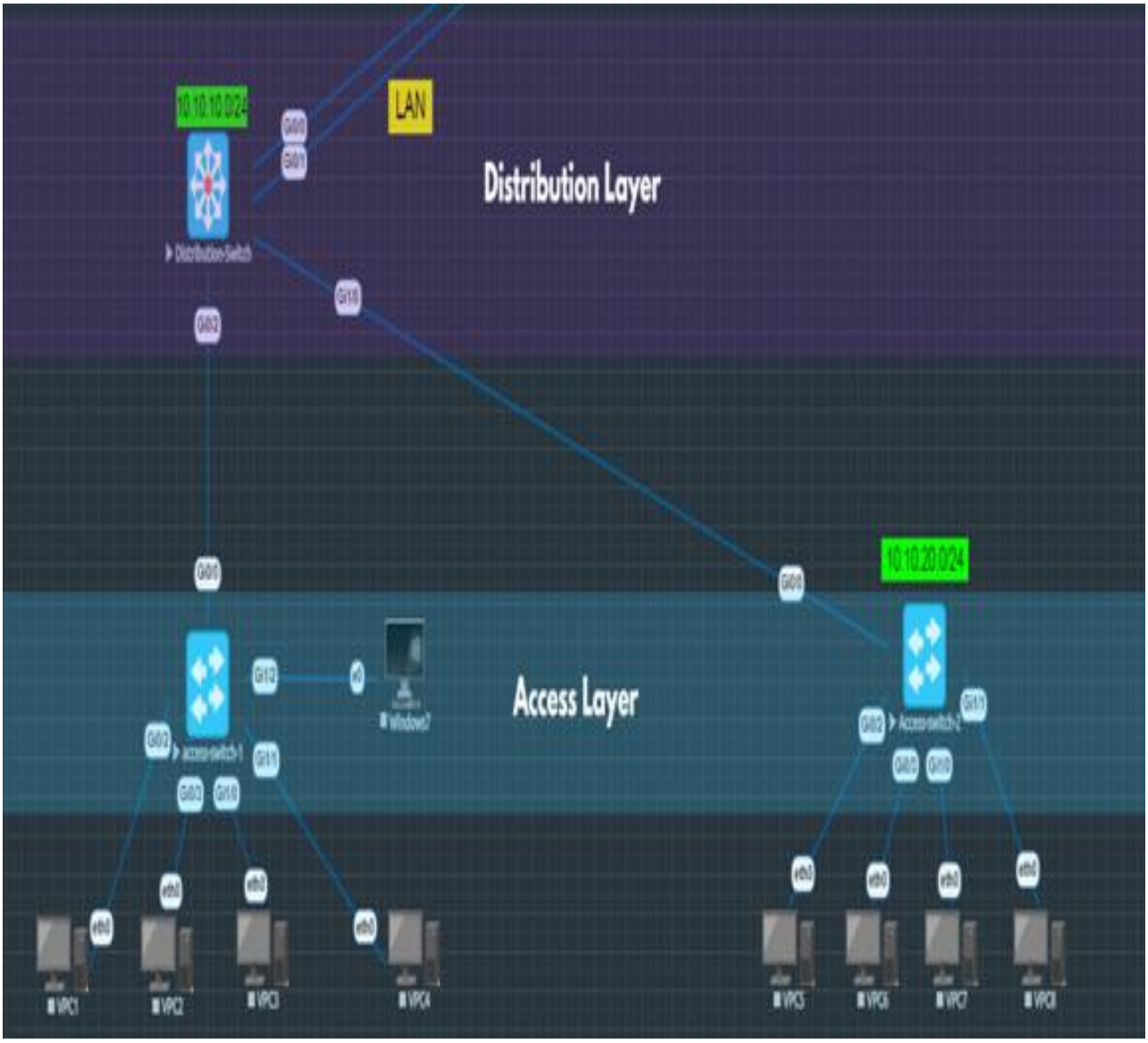

Figure III.3 : Architecture réseau 2 tiers.

III.5.2.Assurer la redondance par des liens multiples

Nous avons assuré une connectivité redondante entre les switch de distribution et FortiGate par le doublement des liens physiques (2 liens) et l'activation de la redondance sur les ports 3 et 4 de FortiGate.

III.6. Plan d'adressage IP

Equipement	connexion	Adresse IP
FortiGate	Management	192.168.2.10/24
	WAN (internet) (Port 2)	10.64.13.10/24
	DMZ (Port 5)	10.10.100.10/24
	VLAN 10	10.10.10.10/24
	VLAN 20	10.10.20.10/24
File-server	Eth0 Connecté avec FortiGate (DMZ)	10.10.100.100/24
Postes (département 1)	DHCP	Range : 10.10.10.2 - 10.10.10.9
Postes (département 2)	DHCP	Range : 10.10.10.2 - 10.10.10.9

Tableau III.1 : Plan d'adressage IP.

III.7. Déploiement de la solution

III.7.1. Modem HUGHES ht 2010 [23]

Dans notre solution nous avons utilisé le modem HUGHES ht 2010 pour fournir un service interne, cela se fait par la connexion d'un modem à un réseau satellitaire de bande Ka. Le port Ethernet du modem se connecte à FortiGate (réseau local).

Le modem est un terminal satellite de nouvelle génération compatible avec le canal de transmission DVB-S2 à large bande offrant la meilleure efficacité à l'industrie. Le canal de retour utilise un codage de parité basse densité puissant et

avancé (LDPC) en conjonction avec la sélection de chemin adaptatif (AIS) pour les meilleures performances de l'industrie.

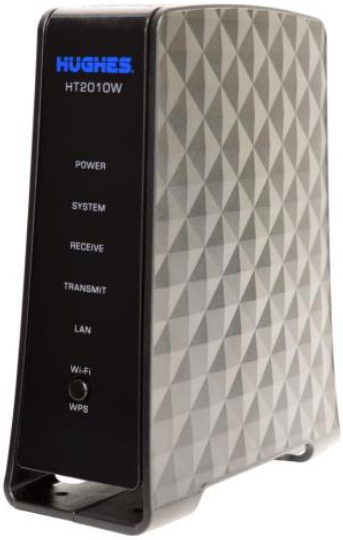

Figure III.4: Modem HUGHES ht 2010.

La figure ci dessous montre l'interface web de ce modem

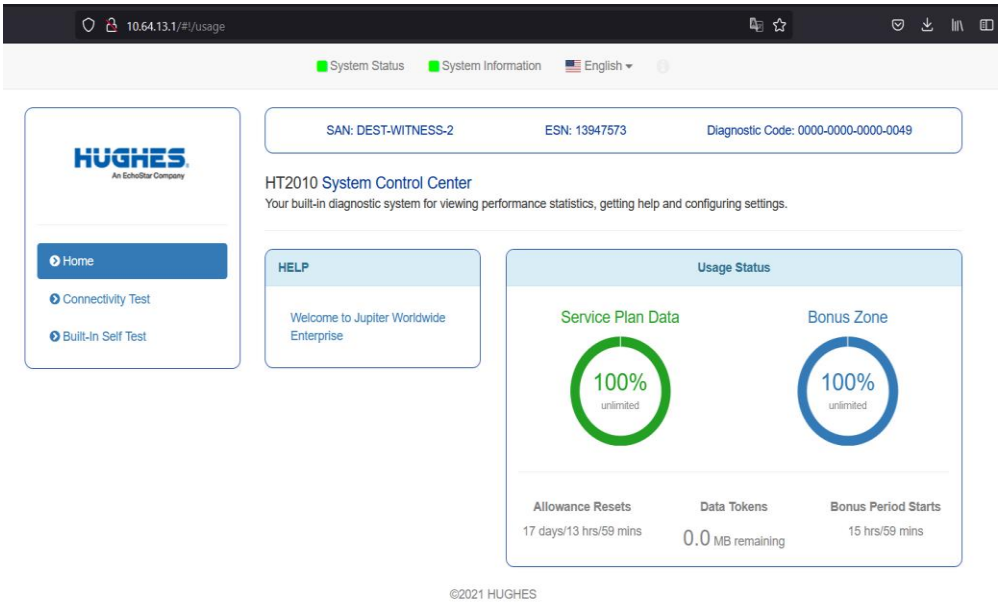

Figure III.5 : Interface web du Modem HUGHES ht 2010**.**

III.7.2.Configuration FortiGate

III.7.2.1. Configuration de l'accès initiale

Pour accéder au http il faut configurer le port management, nous avons utilisé un accès consol.

```
FortiGate-VM64-KVM login: admin
Password:
Welcome!

FortiGate-VM64-KVM # config system interface

FortiGate-VM64-KVM (interface) # edit port1

FortiGate-VM64-KVM (port1) # set mode static

FortiGate-VM64-KVM (port1) # set ip 192.168.2.10/24

FortiGate-VM64-KVM (port1) # set allowaccess http ping

FortiGate-VM64-KVM (port1) # end

FortiGate-VM64-KVM #
```

Figure III.6 : Configuration de l'accès initiale.

III.7.2.2. Configuration des interfaces via GUI (Graphical User Interface)

III.7.2.2.1. Configuration port WAN (Wide Area Network) : Il est relié avec le modem.

- **WAN :** [24] C'est un réseau informatique connectant les sites d'une entreprise entre eux technologie spécifique appelé MPLS (Multiprotocol Label Switching), différente des connexions internet grand public.

- **Objectif de WAN :** [25] Plus puissant que le MAN ou le LAN, le WAN est indispensable au fonctionnement d'internet à l'échelle mondiale car il garantit le maintien d'un réseau informatique sur une très grande surface géographique.

III.7.2.2.2. Configuration port DMZ : Il est relié avec le serveur de fichier.

- **DMZ :** [26] Une DMZ désigne une zone tampon entre le réseau à protéger (votre réseau d'entreprise) et le réseau hostile (internet). Cette zone tampon contient les équipements étant susceptibles d'être accédés depuis Internet.

III.7.2.2.3. Configuration du réseau LAN : Dans cette étape nous avons créé une interface redondante qui regroupe les ports 3 et 4 et après, nous avons créé 2 sous interfaces virtuelle VLAN 10 et VLAN 20.

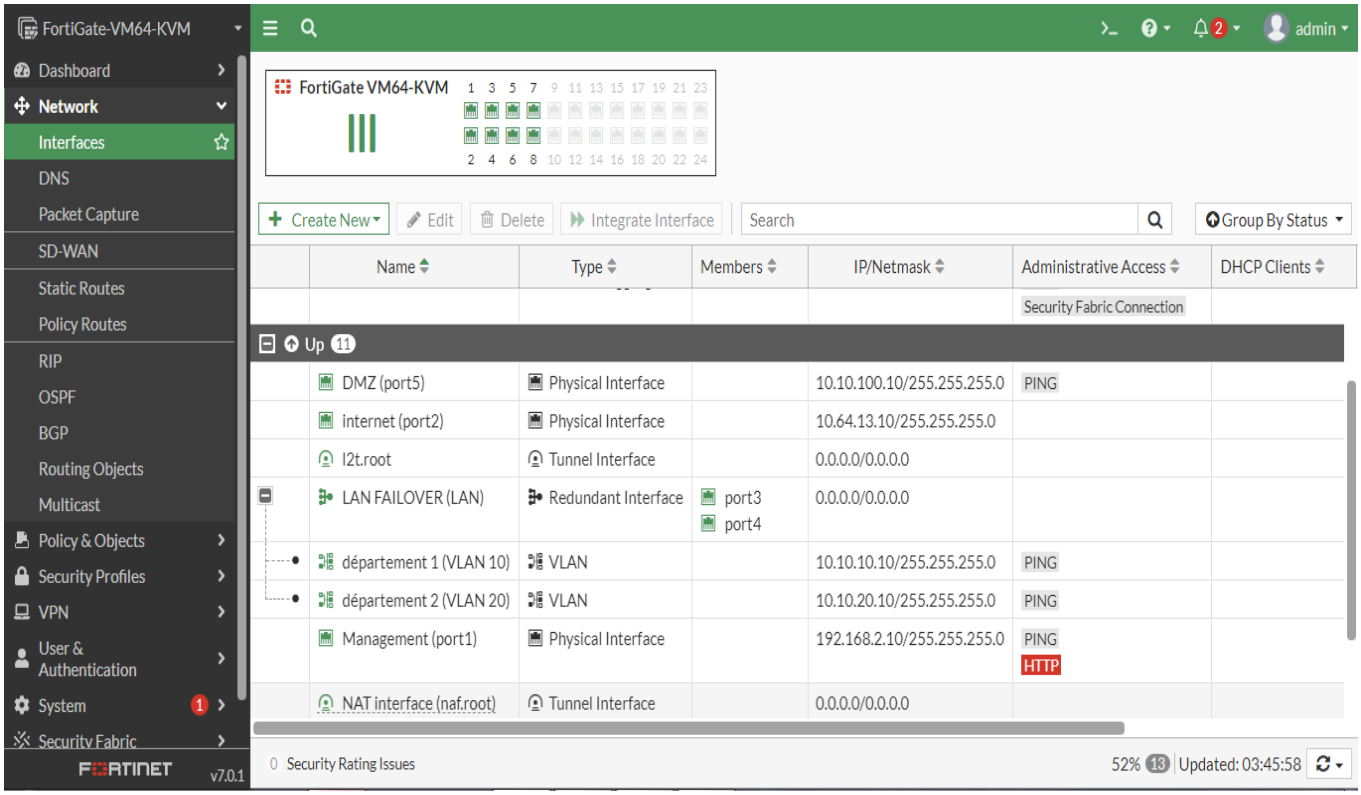

Figure III.7 : Configuration des interfaces via GUI.

- **LAN :** [27] Est un réseau informatique physique ou virtuel. Il permet d'interconnecter par Wifi ou câbles Ethernet des terminaux entre eux. Le LAN peut aussi se connecter à l'extérieur grâce à un accès Internet.
- **Management :** [28] Fait référence à l'administration et à la surveillance des systèmes informatiques d'une entreprise : matériel, logiciel et réseau.
- **L'objectif de management :** [28] C'est un enjeu essentiel, depuis les débuts des systèmes d'information qui peut s'expliquer par l'importance de l'information dans la prise de décision.
- **VPC (Virtual PC) :** Est un PC virtuel avec un système léger qui a des fonctionnalités limitées, utilisé pour des tests du PING, DHCP et DNS.

III.7.2.3. Configuration Switch distribution

Nous avons créé les VLANs 10 et 20 et la configuration des ports Channel sur les liens qui relient les Switch distribution avec FortiGate et le Switch Access.

```
Switch#enable
Switch#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#VLAN 10
Switch(config-vlan)#name departement 1
Switch(config-vlan)#VLAN 20
Switch(config-vlan)#name departement 2
Switch(config-vlan)#end
Switch#
*Oct  5 11:18:14.682: %SYS-5-CONFIG_I: Configured from console by console
Switch#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface range g0/0, g0/1, g0/2, g1/0
Switch(config-if-range)#switc
Switch(config-if-range)#switchport trunk encapsu
Switch(config-if-range)#switchport trunk encapsulation d
Switch(config-if-range)#switchport trunk encapsulation dot1q
Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#end
Switch#
*Oct  5 11:20:01.246: %SYS-5-CONFIG_I: Configured from console by console
```

Figure III.8 : Configuration access distribution.

III.7.2.4. Configuration access switch 1

- Création des vlan (vlan 10 ; vlan 20).
- Configuration des ports trunk (g 0/1).
- Configuration des ports access (g 0/2, g0/3, g1/0, g1/1, g1.2).

```
Switch#enable
Switch#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#VLAN 10
Switch(config-vlan)#name departement 1
Switch(config-vlan)#VLAN 20
Switch(config-vlan)#name derpartement 2
Switch(config-vlan)#end
Switch#
*Oct  5 13:32:42.811: %SYS-5-CONFIG_I: Configured from console by console
Switch#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface g0/0
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
Switch(config-if)#end
Switch#
*Oct  5 13:33:32.143: %SYS-5-CONFIG_I: Configured from console by console
Switch#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface range g0/0?
.  :  <0-7>

Switch(config)#interface range g0/2, g0/3, g1/0, g1/1, g1/2
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access VLAN 10
Switch(config-if-range)#end
Switch#
*Oct  5 13:35:22.408: %SYS-5-CONFIG_I: Configured from console by console
```

Figure III.9: Configuration access switch 1.

III.7.2.5. Configuration access switch 2

- Création des vlan (vlan 10 ; vlan 20).
- Configuration des ports trunk (g 0/2).
- Configuration des ports access (g 0/2, g0/3, g1/0, g1/1).

```
Switch(config)#VLAN 10
Switch(config-vlan)#name departement 1
Switch(config-vlan)#VLAN 20
Switch(config-vlan)#name departement 2
Switch(config-vlan)#end
Switch#
*Oct  5 13:48:12.819: %SYS-5-CONFIG_I: Configured from console by console
Switch#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface g0/0
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
Switch(config-if)#end
Switch#
*Oct  5 13:49:01.123: %SYS-5-CONFIG_I: Configured from console by console
Switch#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface range g0/2, g0/3, g1/0, g1/1
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access VLAN 20
Switch(config-if-range)#end
Switch#
*Oct  5 13:50:35.425: %SYS-5-CONFIG_I: Configured from console by console
```

Figure III.10: Configuration access switch 2.

III.8. Exploitation de la solution

III.8.1. Configuration de l'accès internet

La configuration de l'accès internet se fait sur deux étapes.

- **Première étape :** Nous avons configuré la route par défaut (route statique) pour assurer un acheminement des paquets vers l'internet via l'interface WAN.

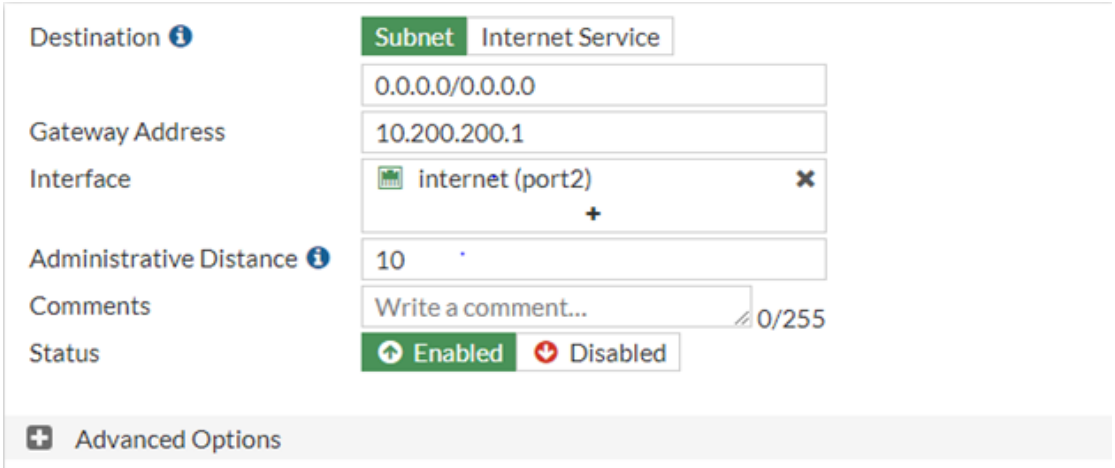

Figure III.11 : Configuration de route statique.

- **Deuxième étape :** Nous avons configuré un rôle (internet access) afin de permettre aux départements d'accéder à l'internet.

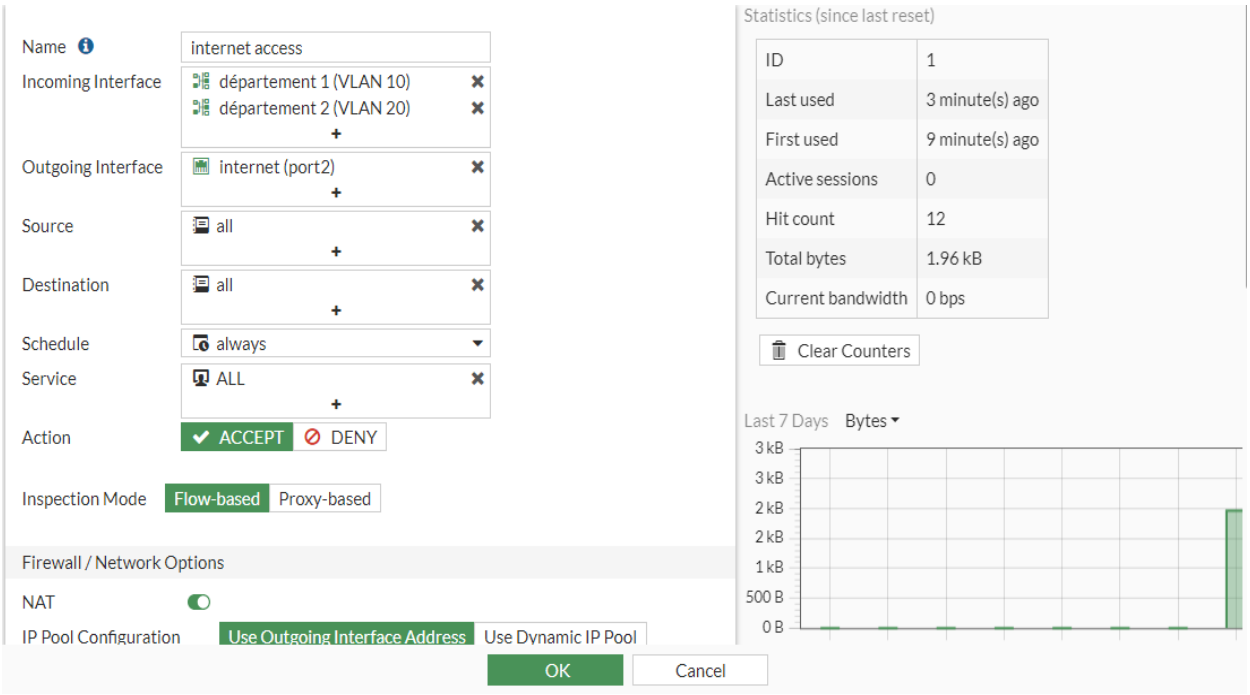

Figure III.12 : Configuration du rôle.

III.8.2. Blocage d'accès aux réseaux sociaux

Le blocage d'accès aux réseaux sociaux se fait sur deux étapes.

- **Première étape :** Nous avons créé un profile de sécurité (web filtre).

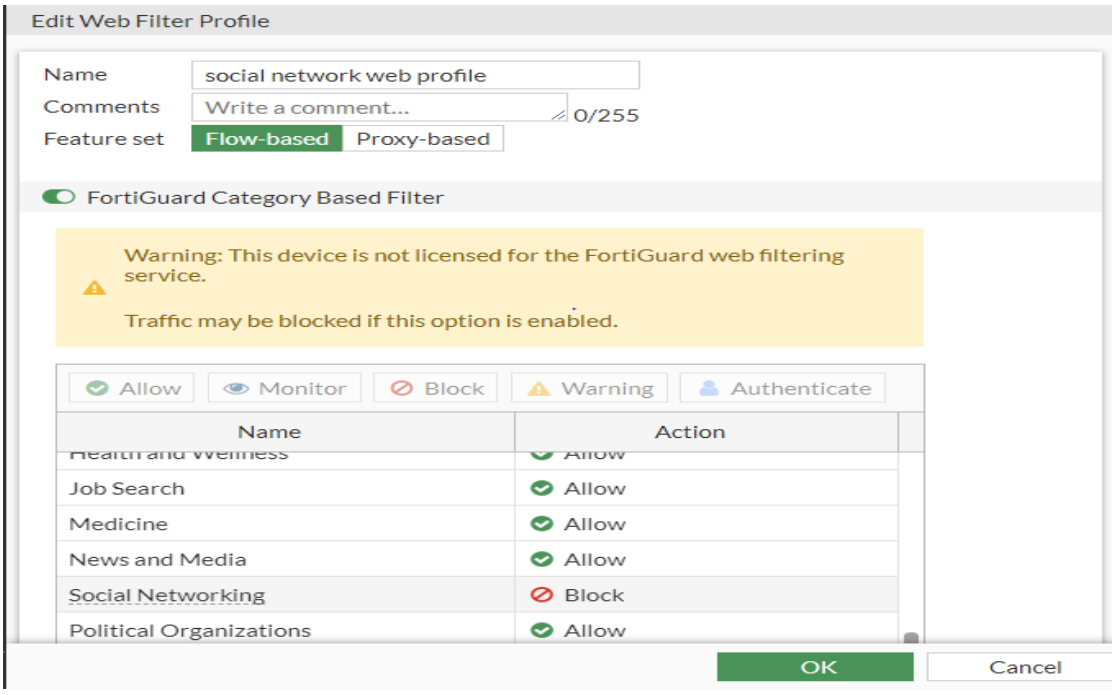

Figure III.13 : Profile de sécurité (security profil).

- **Deuxième étape :** Nous avons appliqué le profile sur le rôle que nous avons déjà créé.

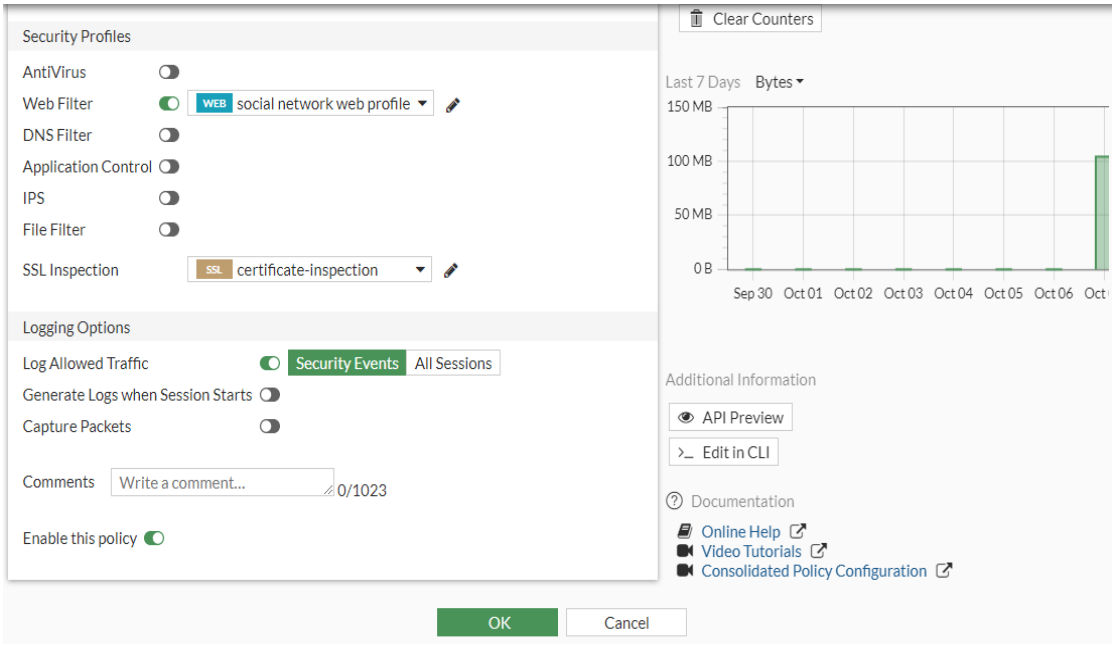

Figure III.14 : Application du profile sur l'accès internet.

III.8.3. Configuration d'un serveur de fichier

Dans cette étape nous avons configuré un serveur de fichier par la création d'un serveur FTP dans la zone DMZ et nous avons configuré des clients FTP sur les deux départements en observant trois étapes :

- **Première étape :** Création d'un serveur FTP.

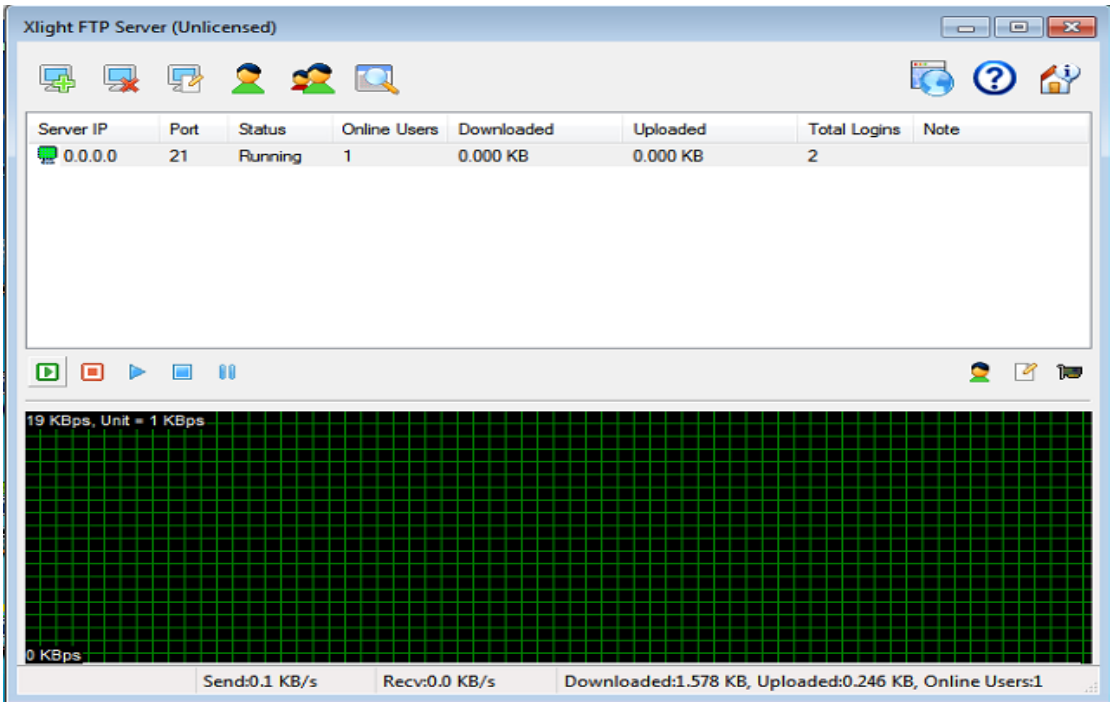

Figure III.15 : Serveur FTP.

- **Deuxième étape :** Installation des clients FTP.

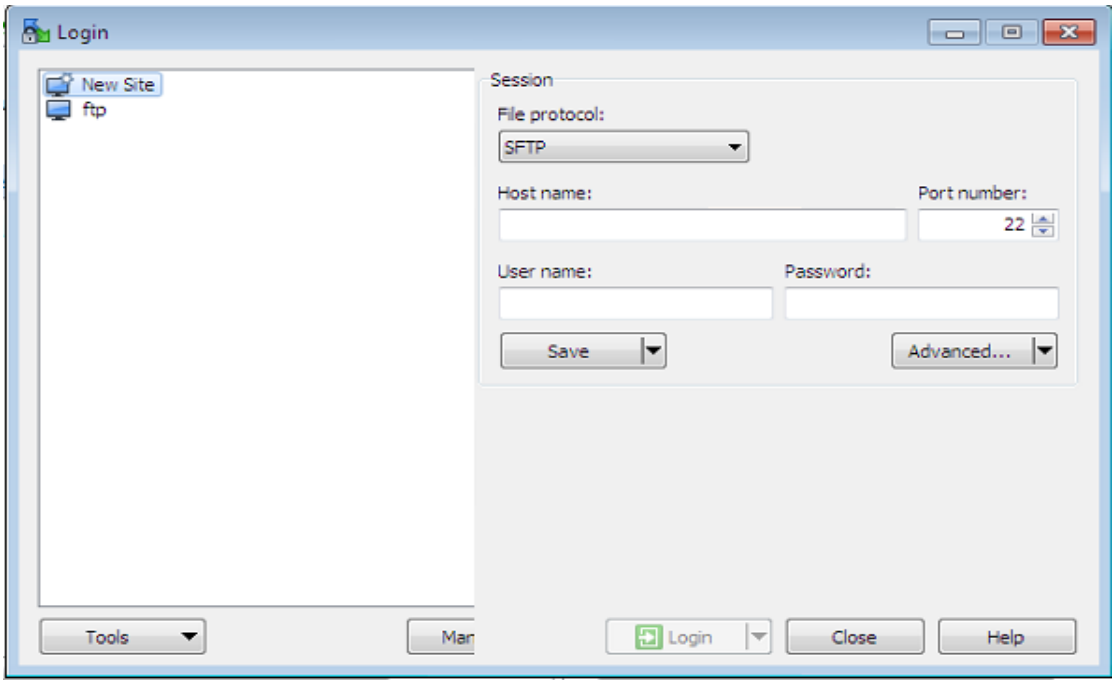

Figure III.16 : client FTP.

- **Troisième étape :** Création d'un rôle qui nous permet d'accéder au serveur FTP (port = 21).

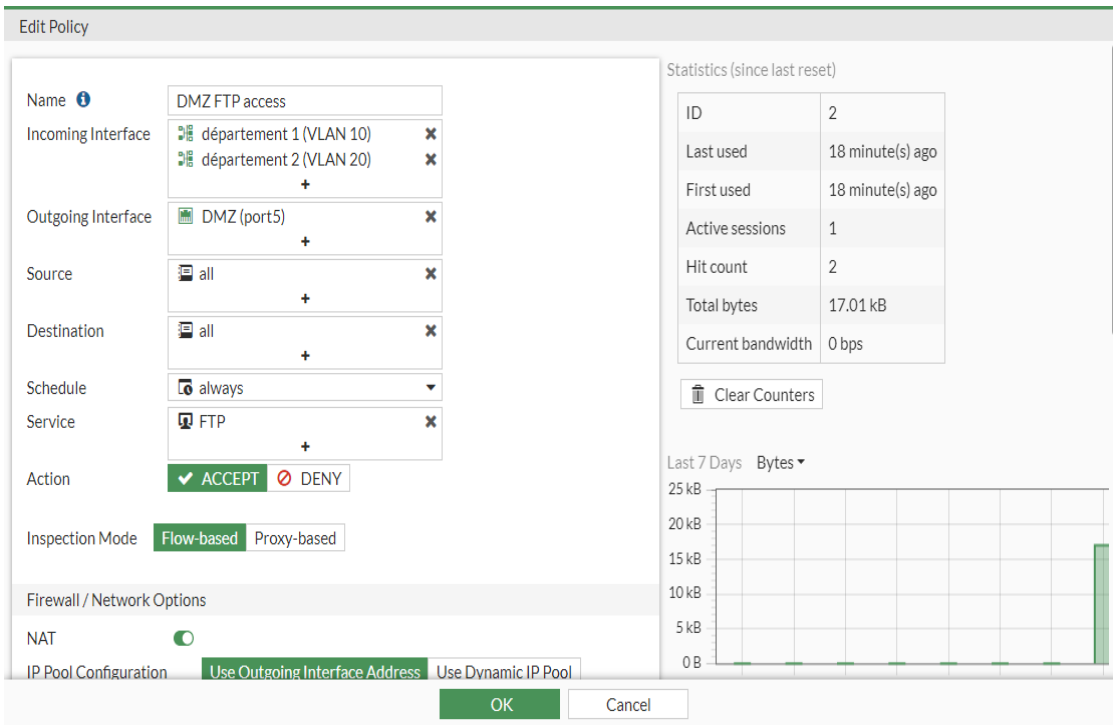

Figure III.17 : Création du rôle.

III.8.4. Automatiser le backup de la configuration FortiGate

Premièrement nous avons créé un nouveau compte utilisateur associé avec un emplacement accessible par les administrateurs uniquement.

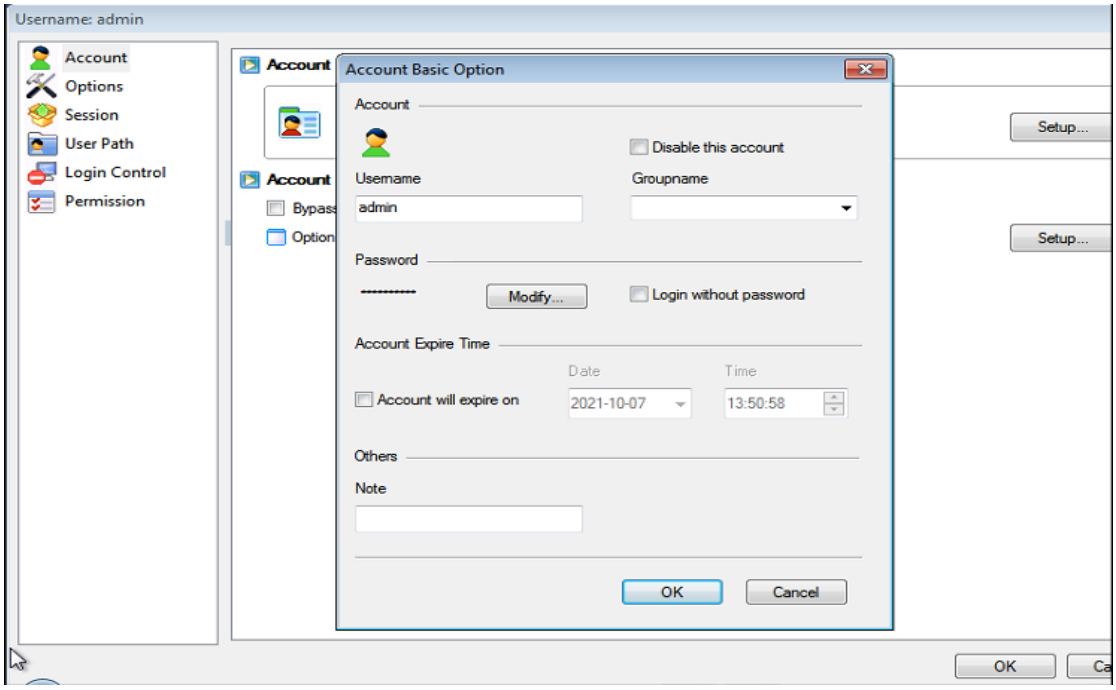

Figure III.18 : Création du compte admin.

Ensuite nous avons procédé à la création d'un point d'automatisation (stitch), celui-ci est composé d'un événement (trigger) et une action.

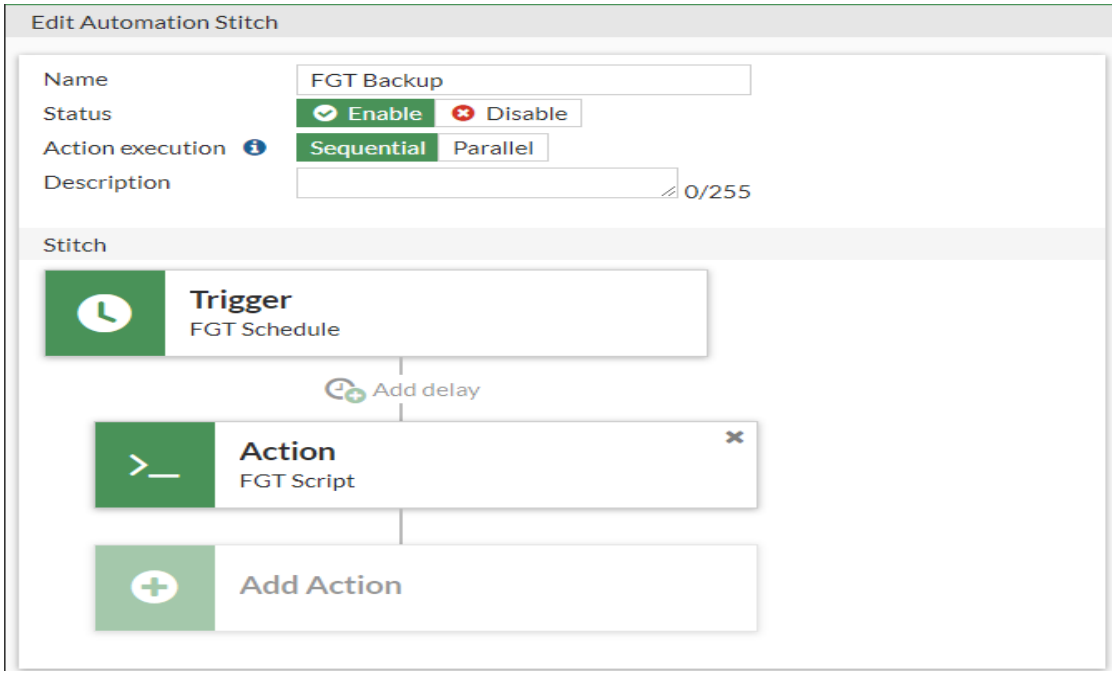

Figure III.19 : Point d'automatisation (stitch).

- **Trigger :** Dans cette partie nous avons mis un événement qui est basé sur le temps (chaque jour à 15 heures).

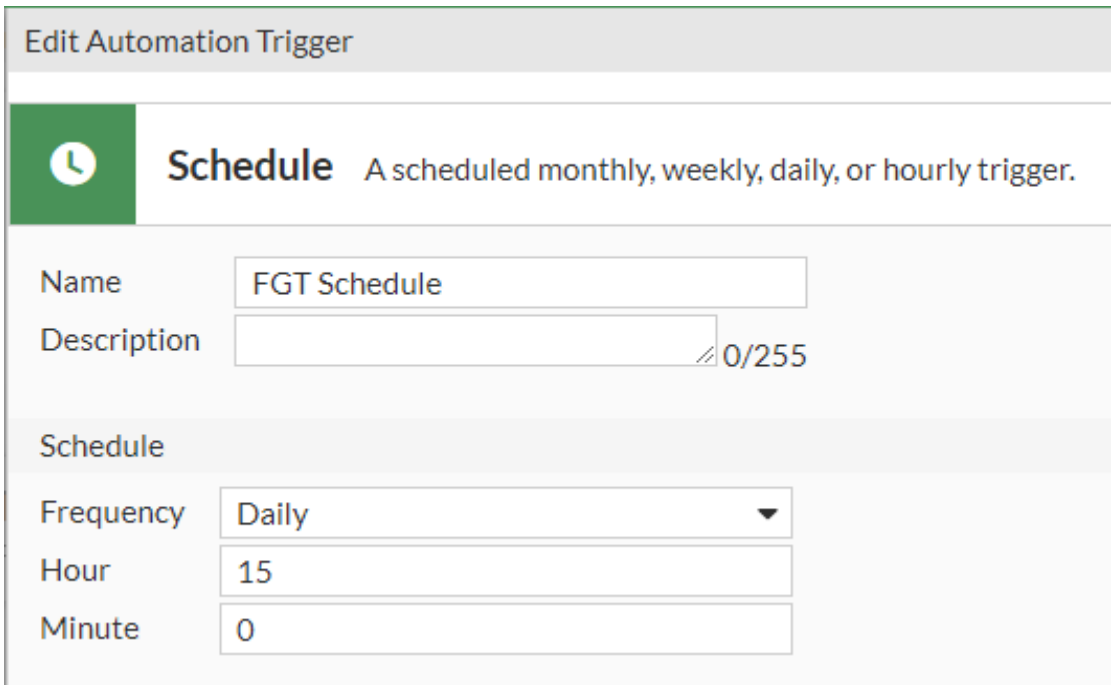

Figure III.20 : Configuration d'un trigger.

- **Action :** Dans cette partie nous avons écrit un script qui fait le backup de la configuration vers le serveur FTP.

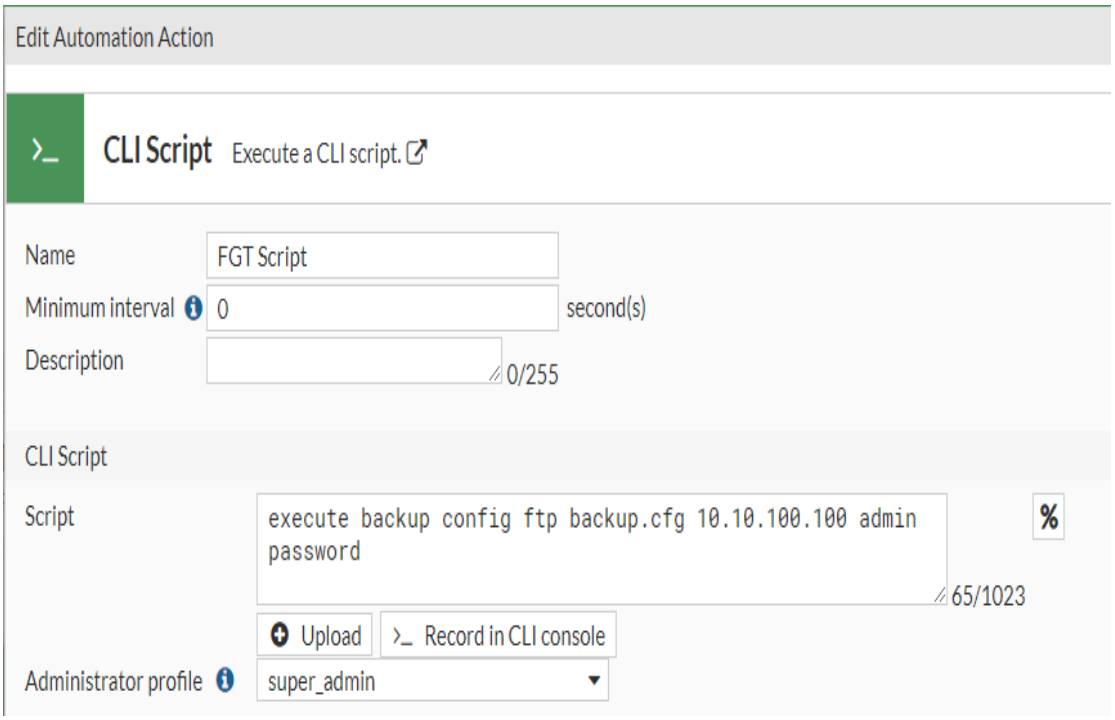

Figure III.21 : Script de la configuration backup.

III.9. Test et résultat

Dans cette étape nous avons fait trois tests :

III.9.1. Test des réseaux sociaux : Nous avons testé l'accès aux quelques sites web qui appartiennent à la catégorie des réseaux sociaux, parmi eux : Facebook.

La figure ci dessous valide l'opération que nous avons faite dans la partie d'exploitation (blocage d'accès aux réseaux sociaux) par un test effectué dans un poste client (département1).

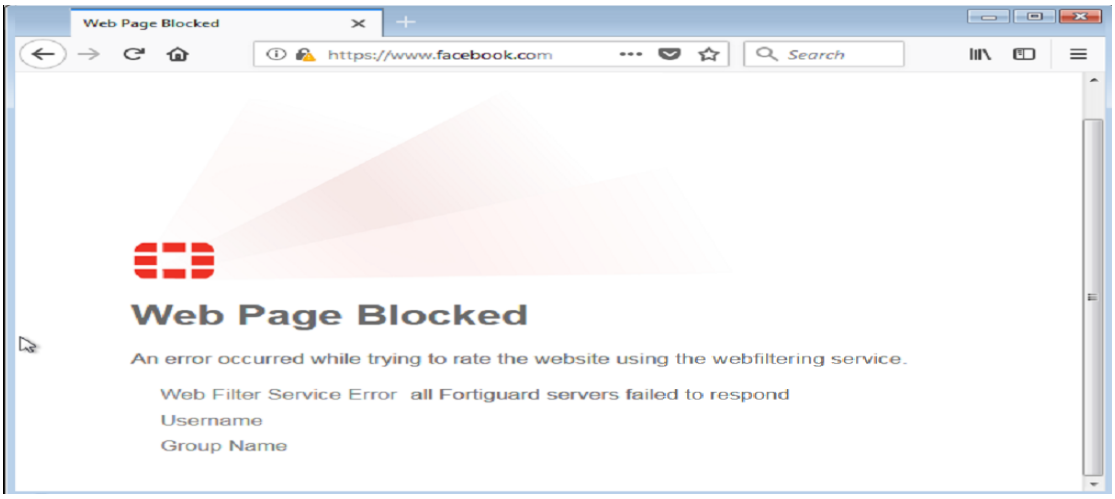

Figure III.22 : Résultat du test Web filtre.

III.9.2. Test FTP : La figure suivante montre la réussite d'accès au serveur de fichier (zone DMZ) via un client FTP installé dans un poste client (département 1).

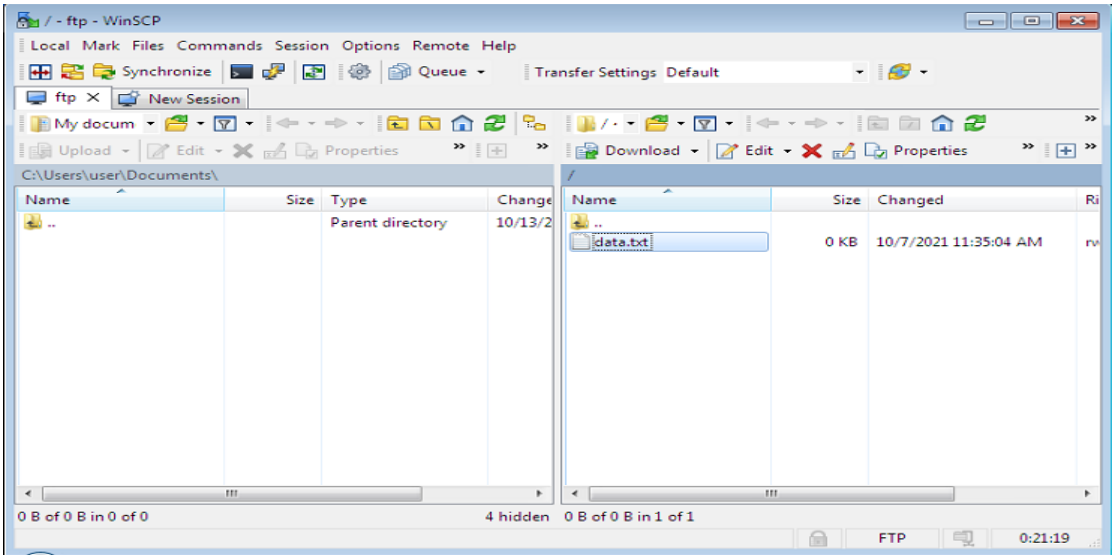

Figure III.23 : Résultat du test FTP.

III.9.3. Test d'automatisation backup : Ce test est approuvé par le paramètre « Trigger Count » qui est incrémenté à chaque fois que l'opération d'automatisation se produit.

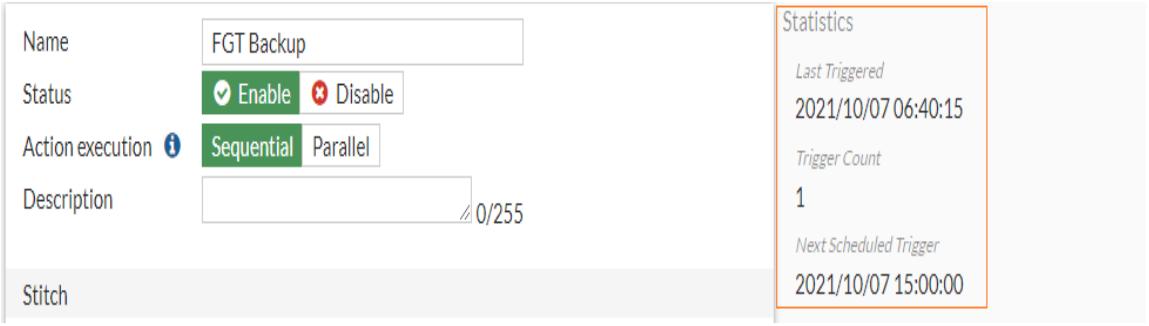

Figure III.24 : Résultat du test backup.

III.9.4. DDoS attaque (Distributed Denial-Of-Service)

Dans ce test nous avons élaboré une attaque DDoS de réseau VLAN 10 (Département-1) vers le serveur de fichiers (Réseau DMZ).

III.9.4.1. Communication TCP

TCP fournit une communication fiable avec ce qu'on appelle un accusé de réception positif avec la retransmission (PAR).

Le client choisit un numéro de séquence initiale, défini dans le premier paquet SYN. Le serveur choisit également son propre numéro de séquence initiale, défini dans le paquet SYN / ACK (montré dans la figure III.25) Chaque côté reconnaît le numéro de séquence de chacun en l'incrémentant: il s'agit du numéro de l'accusé de réception. L'utilisation de séquences et de numéros de l'accusé de réception permet aux deux côtés de détecter des segments manquants ou hors commandements.

Une fois la connexion établie, les ACK suivent le segment et elle se terminera par un RST (Reset) ou FIN.

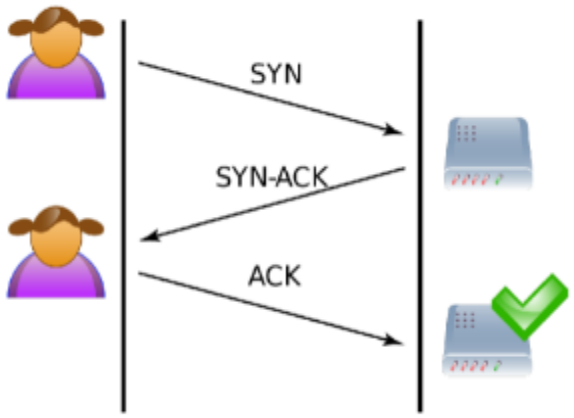

Figure III.25 : Communication TCP.

III.9.4.2. TCP_SYNC_FLOOD

L'attaque DDoS exploite le premier paquet de la communication TCP (TCP_SYNC). Ce type d'attaque génère un grand nombre des paquets de type (TCP_SYNC) nommés « TCP_SYNC_FLOOD » pour consommer des ressources sur le serveur ciblé et le rendre insensible.

Avec SYN Flood DDoS, l'attaquant envoie des demandes de connexion TCP plus rapidement que la machine ciblée ne peut les traiter, provoquant une saturation du réseau.

III.9.4.3. Description de l'attaque

Dans une attaque par inondation SYN (synchronisation), les attaquants envoient une série de paquets SYN légaux avec une fausse adresse IP source au système ciblé. Étant donné que les adresses IP des paquets SYN sont truquées, le paquet SYN-ACK (synchronize-acknowledge) n'arrivera jamais au système ciblé. Ainsi, le système ciblé ne pourra pas établir les connexions.

Le client malveillant n'envoie pas l'ACK (accusé de réception) attendu ou, si l'adresse IP est usurpée, ne reçoit jamais le SYN-ACK en premier lieu. Le serveur attaqué attendra l'accusé de réception de son paquet SYN-ACK pendant un certain temps.

Pendant ce temps, le serveur ne peut pas fermer la connexion en envoyant un paquet RST et la connexion reste ouverte. Avant que la connexion ne puisse expirer, un autre paquet SYN arrivera. Cela laisse un nombre de plus en plus grand de connexions à moitié ouvertes et en effet, les attaques par inondation SYN sont également appelées attaques « semi-ouvertes ». Le système ciblé ne pourra pas accepter de nouvelles connexions TCP. Le service aux clients légitimes sera refusé et le serveur peut même mal fonctionner ou tomber en panne.

III.9.4.4. Analyser l'attaque

Nous avons implémenté un script Python dans la solution qui va produire cette attaque.

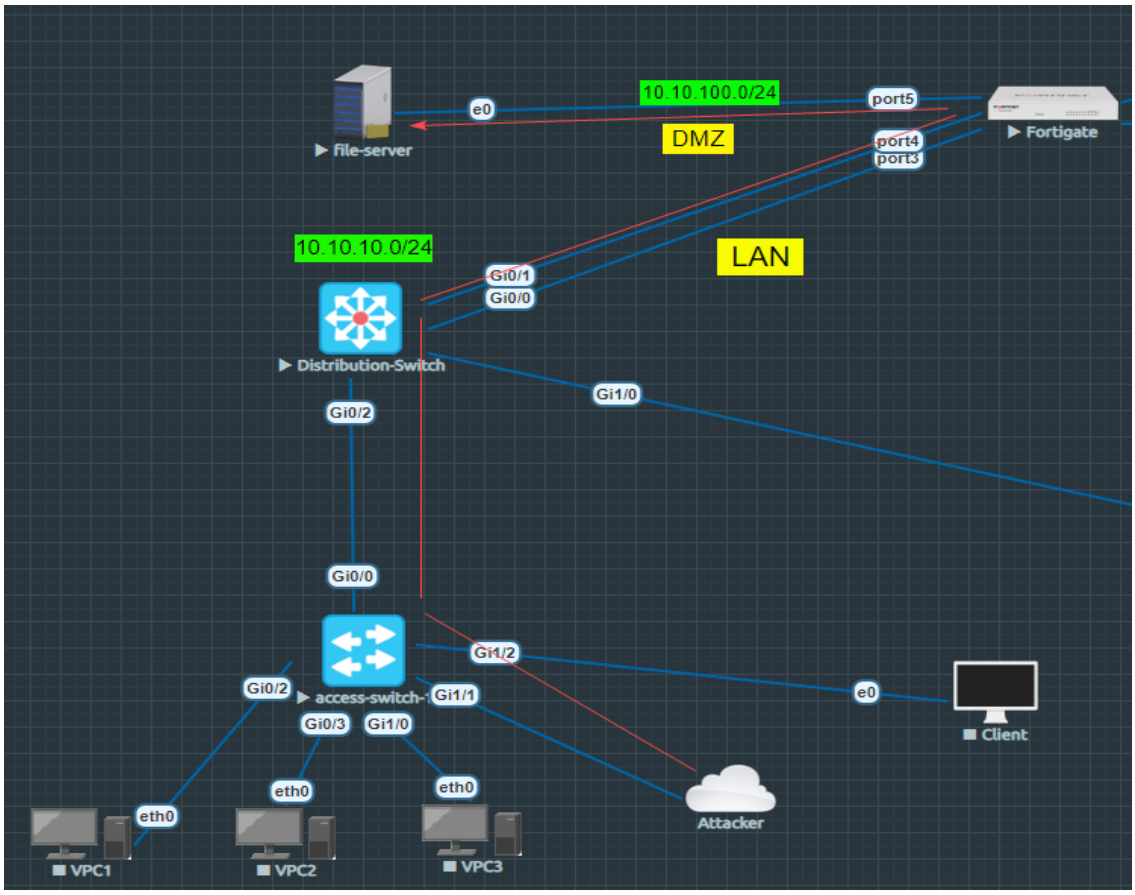

Figure III.26 : Chemin pris par les paquets SYN.

L'attaquant va cibler le serveur du fichier sur le port ouvert 21.

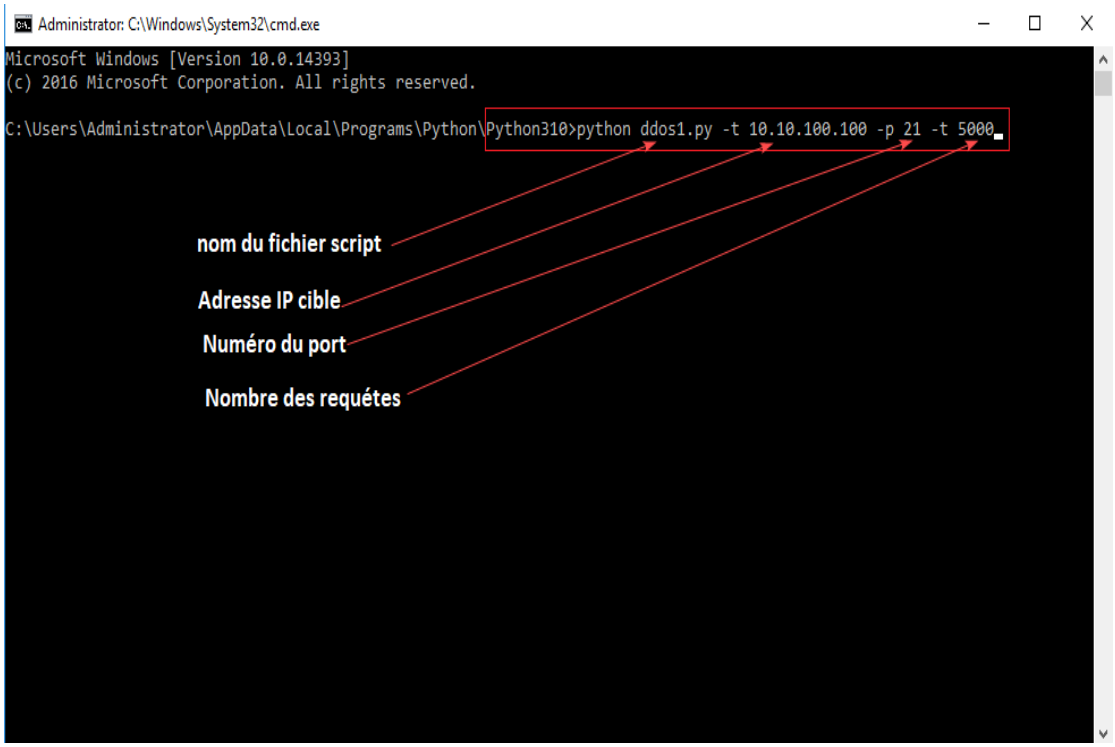

Figure III.27 : Lancement du script Python.

- **Résultat d'attaque :** Le serveur ne répond plus aux requêtes clients.

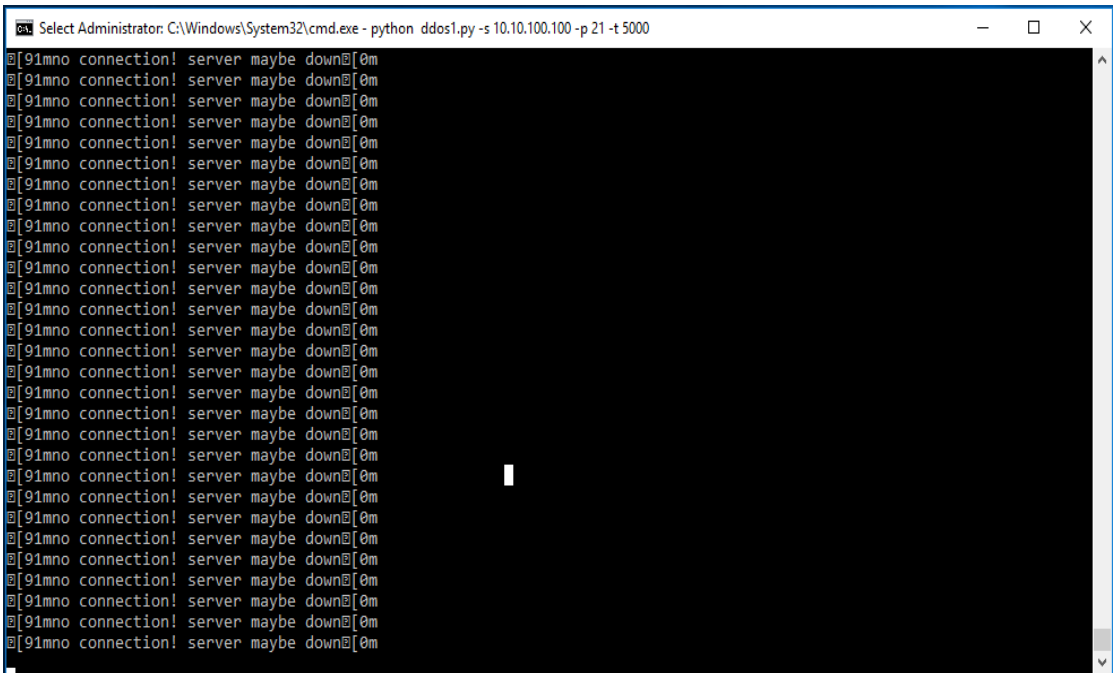

Figure III.28 : Serveur en panne.

La figure ci-dessous montre que le serveur ne répond plus aux requêtes clients à cause des grands nombres des paquets SYN qu'il reçoit.

La création des nombreuses sessions sur FortiGate cause une surcharge sur le CPU (Central Processing Unit) et la RAM (Random Access Memory).

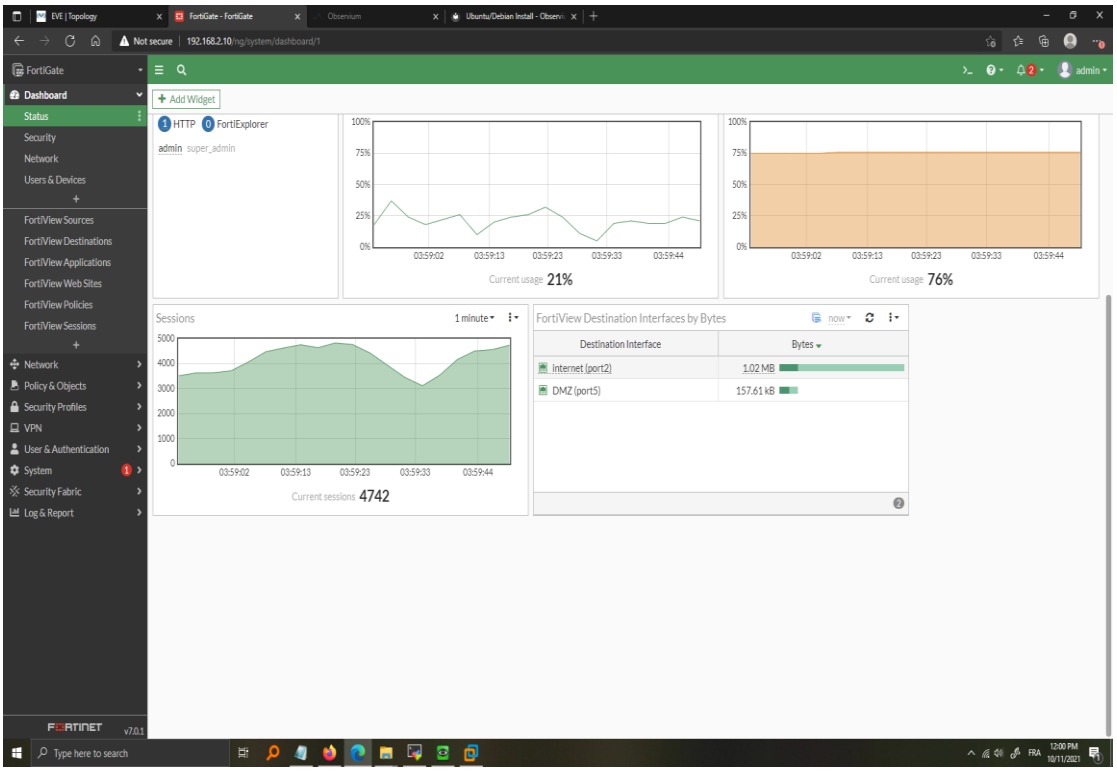

Figure III.29 : Surcharge sur le Firewall.

En outre, on peut voir dans l'interface du serveur de fichier des milliers d'utilisateurs indéfinis affichés.

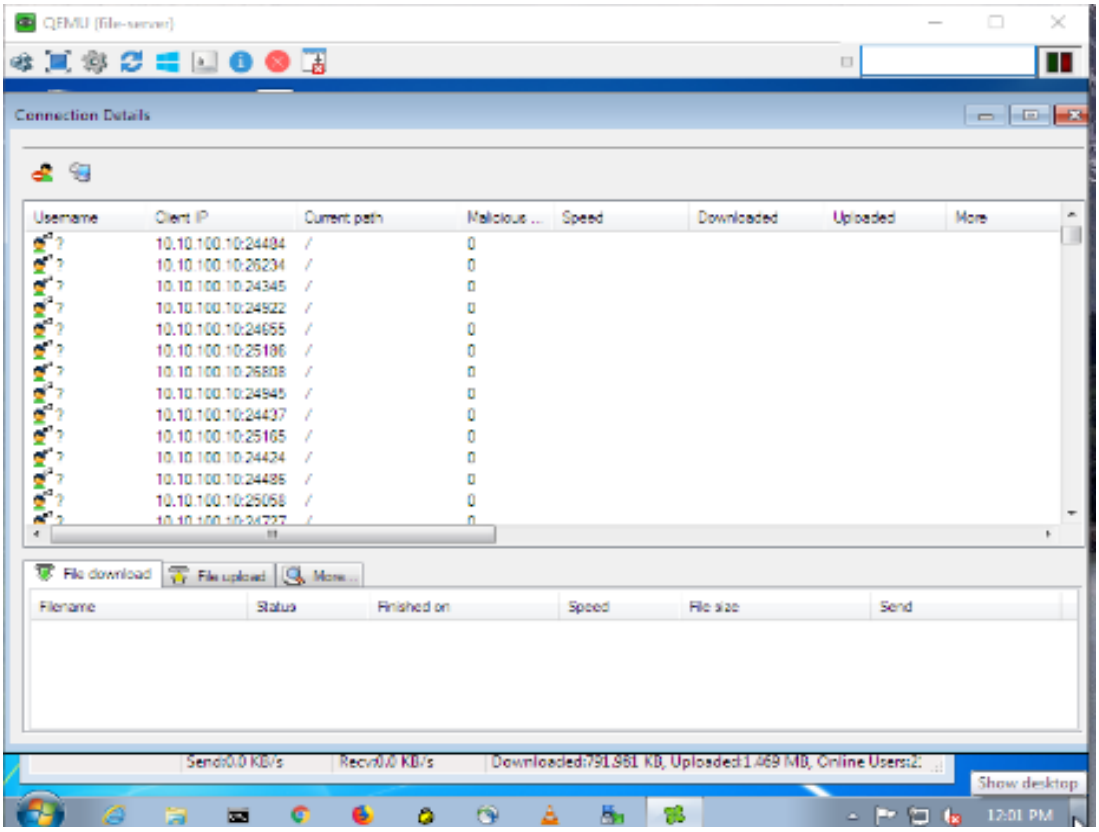

Figure III.30 : Utilisateurs inconnus.

III.9.4.5. Déploiement d'un rôle DDoS IPV4

- Mettre un nom au rôle « DDOS FTP Protect ».
- Choisir l'interface source, les adresses et les services à protéger (on a choisi ALL donc le service FTP est inclus).
- Choisir block pour dropper les paquets selon ses formats (dans notre cas TCP_SYNC_FLOOD).
- Le paramètre threshold signifie le maximum de nombre des requêtes par seconde à accepter, donc un grand nombre des requêtes simultanées signifie une attaque DDOS.
- Activer les logs pour faire des investigations des attaques DDOS.

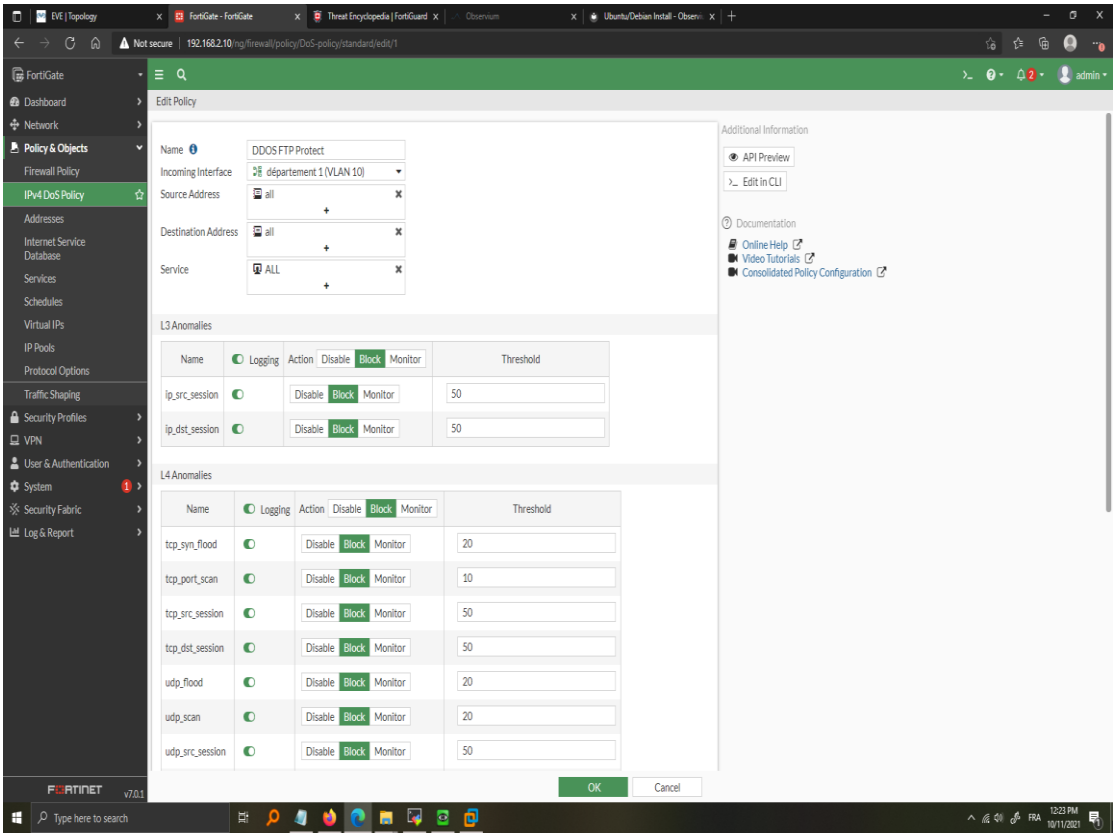

Figure III.31 : Configuration du rôle DDoS.

Après un autre lancement de l'attaque, nous voyons sur les logs (la source et les types des paquets). Pour confirmer, nous observons le paramètre TCP_SYNC_FLOOD qui a été généré par un client tenant l'adresse IP 10.10.10.5

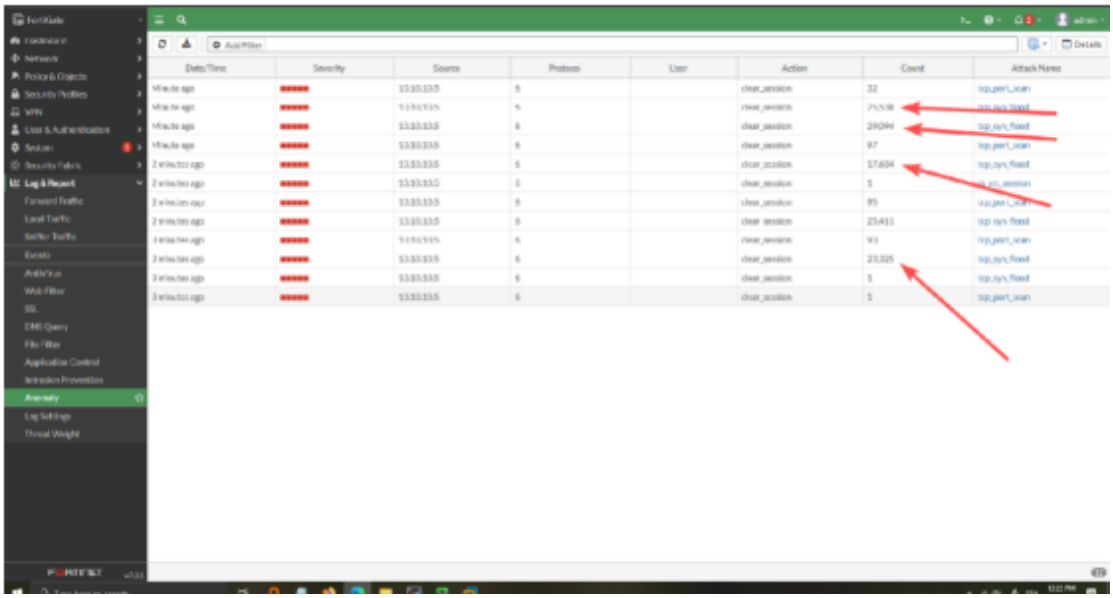

Figure III.32 : Paramètre TCP_SYNC_FLOOD.

Comme montre la figure ci-dessous, le firewall n'est pas affecté par l'attaque.

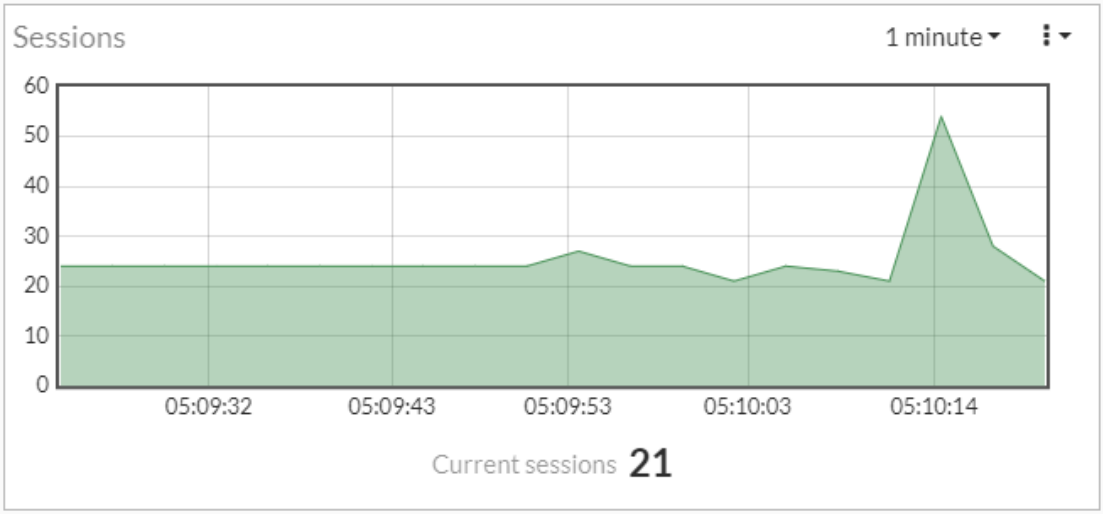

Figure III.33 : Firewall dans l'état normal.

On peut voir aussi que le serveur du fichier ne reçoit pas des paquets indéfinis créé par l'attaquant.

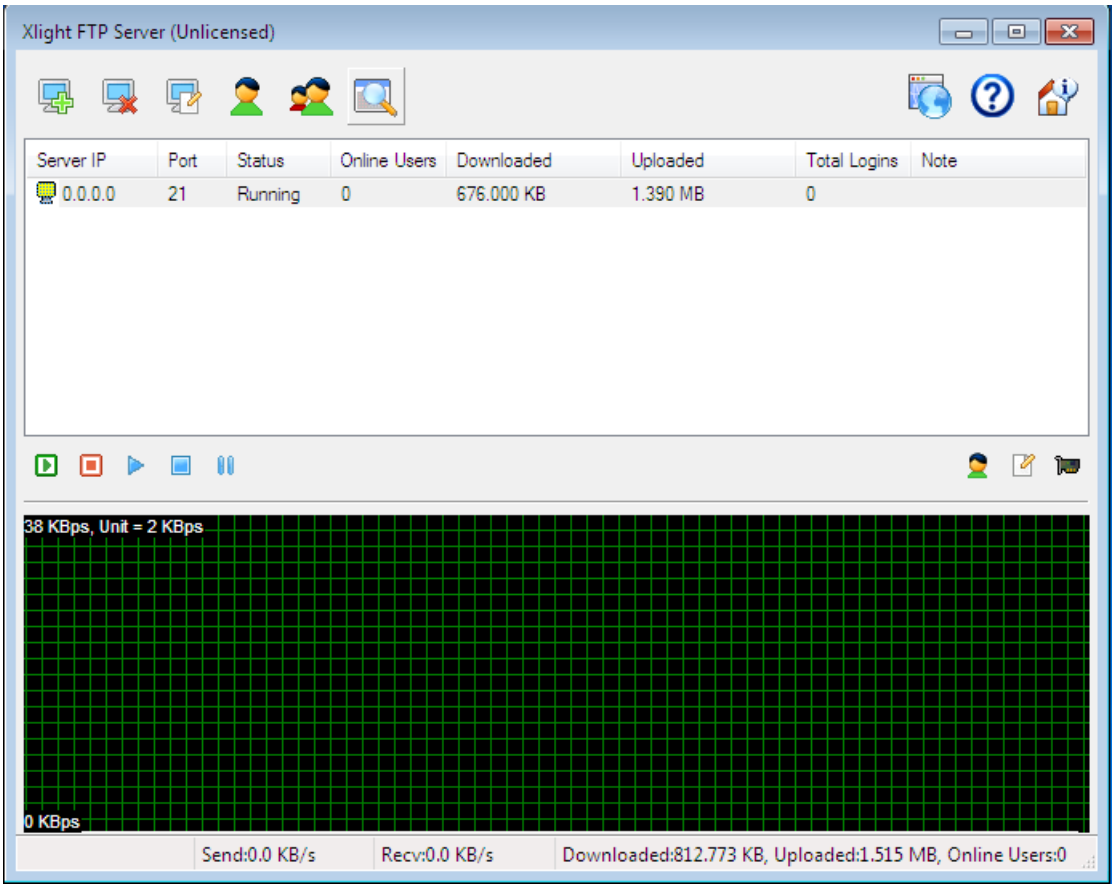

Figure III.34 : Serveur FTP marche normal.

Conclusion

Dans ce chapitre nous avons déployé un réseau LAN sécurisé contre les intrus de l'environnement externe et les attaques potentielles de l'environnement interne par le déploiement des différents rôles et profiles. Le réseau déployé est fortement optimisé grâce à sa conception (architecture 2 tiers) et des VLANs créés qui réduisent la circulation des paquets de diffusions et redondants grâce aux liens physiques multiples.

Conclusion générale

Conclusion générale

Le travail que nous avons présenté dans ce mémoire consiste à étudier la mise en place d'un réseau LAN sécurisé du système VSAT via FortiGate.

Pour ce faire, nous avons réalisé un stage pratique au sein d'Algérie Télécom Satellite (ATS) de LAKHDARIA wilaya de Bouira.

A signalé que l'Algérie Télécom Satellite est un organisme étatique spécialisé dans les télécommunications doté d'un matériel très sophistiqué et d'un encadrement professionnel. Ceci nous a permis de mener à bien ce présent travail.

Au cours de ce stage nous avons pu utiliser l'architecture 2 tiers qui garantie une cohérence des données dont la sécurité est assuré par l'utilisation d'un pare-feu nouvelle génération (FortiGate).

Afin de démontrer la fiabilité de FortiGate, nous avons déployé une solution pour sécuriser le réseau LAN. Le réseau sécurisé est basé sur le déploiement de la solution étudiée et l'exploitation de cette dernière.

Les tests effectués confirment que la solution proposée pour sécuriser un réseau LAN est satisfaisante. En effet, des vérifications pratiques ont démontré le blocage d'accès aux réseaux sociaux (voir figure III.22 P48), la réussite d'accès au serveur de fichier (zone DMZ) via un client FTP installé dans un poste client (voir la figure III.23 p48), la réalisation d'une sauvegarde automatique sécurisée (voir figure III.24 p49) et la sécurisation d'un serveur contre l'attaque DDoS (voir la figure III.34 P55).

Cependant, il est souhaitable de saisir cette perspective de recherche pour développer d'avantage ce présent travail afin de trouver des techniques de sécurisation de réseaux sans fil via FortiGate sans passer par un réseau LAN.

Références bibliographiques

[1] Philippe ATELIN, Réseaux informatiques : notions fondamentales, 3eme édition, édition ENI, janvier 2009.

[02] José DORDOIGNE, Réseaux informatiques : notions fondamentales, 7eme édition, édition ENI.

[03] Sharles M.Kozierok, TCP/IP guide: a comprehensive, illustrated internet protocols reference, 2005.

[04] Malek RAHOUAL, Patrick SIARRY, Réseaux informatiques : conception et optimisation, édition TECHNIP, Paris, France, 2006.

[05] Cyrille DUFRESNES. Pare-feu-Proxy-DMZ, http://notionsinformatique.free.fr, consulté le 08/06/2008.

[06] introduction aux réseaux TCP/IP, institut universitaire de technologie d'Amiens, support de cours 1998/99 réseaux et télécom.

[07] Jie Wang, Computer Network Security Theory and Practice, 2008.

[08] https://www.pandasecurity.com , consulté le 27/07/21.

[09] Mark Ciampa, Ph.D. livre compTIA secutry +guide to network security fundamentals, fifth edition.

[10] A. ALTUNAIJI, " Mise en place d'un réseau sécurisé sous linux", Université Claude Bernard, Lyon 1, France, novembre 2002.

[11] http://cours-informatique-gratuit.fr, consulté le 10/07/2021.

[12] Joe Friedman foreword by Bassam Khan, Definitive Guide to Complete Network Visibility, Gigamon, 2019_2020.

[13] A. MARACON, B. FABREJON " Les Firewalls - La sécurité des réseaux ", Eyrol, 1999.

[14] Cyrille DUFRESNES. Pare-feu-Proxy-DMZ, http://notionsinformatique.free.fr, 08/06/2008.

[15] T. KOUASSI. Mémoire sur Etude et optimisation du réseau locale de inova si. Centre d'expertise et de perfectionnement en informatique, Abidjan - Ingenieur, 2007.

[16] https://community.jisc.ac.uk/library/advisory-services/modes-firewall-operation, consulté le 11/07/2021.

[17] https://help.stonesoft.com/onlinehelp/StoneGate/SMC/6.4.0/GUID-6A7AECF5-626D-4722-96F6-510B60AE7427.html, consulté le 14/07/2021.

[18] https://help.stonesoft.com/onlinehelp/StoneGate/SMC/6.4.0/GUID-6A7AECF5-626D-4722-96F6-510B60AE7427.html, consulté le 14/07/2021.

[19] Gérard MARAL, VSAT Networks, 2 eme édition, 2003.

[20] Jean Buet, Philippe Durance, VSAT : les réseaux satellites d'entreprise, applications et sécurité, 1996.

[21] Rajpreet Kaur, Adem Hils, Jeremy D'Hoinne, Gartner Magic Quadrant Network Firewells, 09 November 2020.

[22] Uldis Dzerkals, Michael Doe, Christopher Lim, EVE-NG professional cookbook, version 1.0.

[23] **[**HT 2010 Wifi Routeur Satellite, HUGHES An Echostar Company, juillet 2018.

[24] http://www.pyxya.fr, consulté le 01/10/2020.

[25] https://www.journalduner.fr, consulté le 01/10/2020.

[26] http://assistancepro.orange.fr, consulté le 01/10/2020.

[27] http://www.bouyguestelecom-entreprises.fr, consulté le 01/10/2020.

[28] http://actualiteinformatique.fr, consulté le 01/10/2020.

Résumé

FortiGate est devenu parmi les meilleurs outils de protection contre les malwares. Il est efficace pour protéger toutes les bordures des réseaux. L'objectif de ce travail est la mise en place d'un réseau LAN sécurisé du système VSAT via FortiGate comme solution.

Le pare-feu NG permet de contrôler le flux d'informations qui circule entre un ordinateur et un réseau internet. Parmi les fonctionnements que nous avons vus : bloquer l'accès aux réseaux sociaux pour les départements, accéder aux serveurs du fichier par un client FTP dans la zone DMZ, automatiser le backup de la configuration FortiGate et la sécurisation d'un serveur contre l'attaque DDoS.

Mots clés : FortiGate, Malwares, pare-feu, réseau, DMZ, FTP.

Abstract

FortiGate has become the best malware protection tool, it is effective in protecting all edges of networks. The objective of this work is the establishment of a secure LAN network of the VSAT system via FortiGate as a solution.

This NG firewall controls the flow of informations that circulates between a computer and Internet network. Among the operations we have seen: block access to social networks for department, access to file servers by an FTP client in the DMZ zone, automated backup of the FortiGate configuration and the securing of a server against the DDoS attack.

Keywords: FortiGate, Malware, Firewall, Network, DMZ, FTP.

الملخص

أصبح FortiGate أفضل أداة للحماية من البرامج الضارة ، فهو فعال في حماية جميع حواف الشبكات. الهدف من هذا العمل هو إنشاء شبكة LAN آمنة لنظام VSAT عبرFortiGate كحل. يتحكم جدار الحماية في تدفق المعلومات التي تنتشر بين الكمبيوتر وشبكة الإنترنت. من بين العمليات التي رأيناها: حظر الوصول إلى الشبكات الاجتماعية للأقسام، والوصول إلى خادم الملفات بواسطة عميل FTP في منطقة DMZ والنسخ الاحتياطي التلقائي لتكوين FortiGate, وتأمين الخادم ضد هجوم DDoS.

الكلمات المفتاحية : FortiGate ،البرامج الضارة ، جدار الحماية، شبكة الاتصال، FTP ، DMZ