REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA

RECHERCHE SCIENTIFIQUE

UNIVERSITE M'HAMED BOUGARA BOUMERDES
FACULTE DE TECHNOLOGIE

Domaine : Sciences et Technologies

Filière : Télécommunications

Mémoire de projet de fin d'études pour l'obtention du Diplôme de Master

Spécialité : Réseaux et Télécommunications

Présenté par : Fareseddine MEKIRI

Thème

Renforcement de la sécurité du réseau de la Direction Générale NESDA via FireWall

---

Soutenu le 26/06/2024

Devant le jury composé de :

GUERBAI	Yasmine	MCB	UMBB	Président
BELAOURA	Widad	MCB	UMBB	Examinateur
MAHDI	Ismahan	MCB	UMBB	Superviseur
HEBABCHA	Kamel	Directeur informatique	DG Nesda	Co encadrant

Année universitaire : 2023/2024

Remerciements

Nous tenons tout d'abord à exprimer notre profonde gratitude à Allah, qui nous a accordé la force et le courage nécessaires pour mener à bien nos études et réaliser ce modeste travail.

Nous souhaitons exprimer nos sincères remerciements à tous les enseignants du département de Génie Électrique qui ont contribué à notre formation tout au long de notre parcours universitaire. En particulier, nous tenons à remercier chaleureusement notre promotrice, Docteur Ismahan MAHDI, maître de conférences et chercheur à l'Université M'hamed Bougara. Sa patience, sa disponibilité et ses précieux conseils ont grandement nourri notre réflexion.

Nous tenons également à exprimer notre reconnaissance envers l'ensemble du personnel d'e la direction générale NESDA pour nous avoir accueillis au sein de leur entreprise.

Nous adressons nos sincères remerciements aux membres du jury d'avoir accepté d'examiner et d'évaluer notre travail.

Nous souhaitons exprimer notre profonde gratitude envers nos familles et nos amis(es) pour leur soutien et leurs précieuses contributions tout au long de notre parcours académique.

Enfin nous tenons à exprimer notre reconnaissance et notre gratitude à tous ceux qui ont contribué à notre réussite de près ou de loin. Votre soutien inestimable et votre présence ont été une source de motivation et d'inspiration.

Dédicace

Je dédie ce travail qui n'aurait jamais pu voir le jour sans le soutien indéfectible et sans limite

De mes chers parents qui m'ont soutenu surtout avec leur Dou3a jour et nuit

Pour qu'ils me voient au sommet et comme une étoile, à la source de la

Douceur.

Leur amour et leur soutien inconditionnel ont été essentiels pour que

J'atteigne le stade où je me trouve aujourd'hui. Que Dieu les protège et que la réussite

Continue de se présenter à moi, afin de pouvoir les combler de bonheur.

Table des matières

Liste des figures

Listes des tableaux

Liste des abréviations

AD DS:	Active Directory Domain Services
ACL:	Access control list
BEC:	Business Email Compromise
BLOB:	Binary Large Object
DoS :	Denial-of-service
DC:	Domain controller
DNS:	Domain name system
DHCP :	Dynamic Host Configuration Protocol
DMZ:	Demilitarized zone
DNAT:	Destination Network Address Translation
DLP:	Data loss prevention
DDoS:	Distributed denial-of-service
ESA:	Email Security Appliance
FTP:	File transfer protocol
HTTP:	Hyber text transfer protocol
IPSec:	Internet Protocol Security
IPS:	Intrusion prevention system
IP:	Internet protocol
ICMP:	Internet Control Message Protocol
LDAP:	Lightweight Directory Access Protocol
LAN:	Local area network
MAC:	Media access control
MITM:	Man-in-the-middle

NGFW:	Next Generation Firewall
NAT:	Network address translation
NACLs:	Network access control lists
P2P:	Poste à poste
SGBD:	Systeme de Gestion de Base de Donnée
SQL:	Structured Query Language
SSH:	Secure Shell
SMB:	Server message block
SSL:	Secure Sockets Layer
SMTP:	Simple Mail Transfer Protocol
TCP:	Transmission Control Protocol
TIs :	Technologies de l'information
TLS:	Transport Layer Security
UDP:	User Datagram Protocol
URL:	Uniform Resource Locator
WAF:	Web Application Firewall
WAN:	Wide area network
VIP:	Virtual ip
VPN:	Virtual privat network
XSS:	Cross-site scripting

ملخص

أمن تكنولوجيا المعلومات هو عملية حماية أصول تكنولوجيا المعلومات الخاصة بالمؤسسة، مثل الأنظمة والشبكات والأجهزة الرقمية والبيانات، من الوصول غير المصرح به وخروقات البيانات والهجمات الإلكترونية1. ويشمل تدابير مثل نقطة النهاية والسحابة والشبكة وأمن التطبيقات. يمكن أن تكون تكاليف خروقات البيانات كبيرة ، مما يؤثر على الإيرادات والسمعة ويؤدي إلى غرامات وخسائر في الأصول. في هذا السياق ، قمنا بتطوير حلنا الخاص ، والذي تم تكييفه خصيصا لاحتياجات الشركة. يتميز المشروع بنهج محسن وفعال من حيث التكلفة ودقيق لتعزيز أمن المؤسسة وتحسين الأداء العام للشبكة

الكلمات المفتاحية:تفويض، حركة المرور، الهجمات IPS,WAF،DMZ،FortiGate، جدار الحماية، أمن الشبكات

Résumé

La sécurité informatique consiste à protéger les actifs informatiques d’une organisation, tels que les systèmes, les réseaux, les appareils numériques et les données, contre les accès non autorisés, les violations de données et les cyberattaques1. Elle englobe des mesures telles que la sécurité des terminaux, du cloud, du réseau et des applications. Les coûts des violations de données peuvent être considérables, affectant le chiffre d’affaires, la réputation et entraînant des amendes et des pertes d’actifs.C'est dans ce contexte que nous avons entreprise le développement de notre propre solution, spécifiquement adaptée aux besoins de l’entreprise. Ce projet se distingue par une approche optimisée, économique et précise, permettant de renforcer la sécurité d'entreprise et optimiser d'une maniére générale les performances de réseau.

Mots clés : Pare-feu, Sécurité réseau, FortiGate, DMZ, IPS,WAF,Autorisation, trafics, attaques

Abstract

IT security is the process of protecting an organization's IT assets, such as systems, networks, digital devices, and data, from unauthorized access, data breaches, and cyberattacks1. It encompasses measures such as endpoint, cloud, network, and application security. The costs of data breaches can be considerable, affecting revenue, reputation, and resulting in fines and asset losses. It is in this context that we have undertaken the development of our own solution, specifically adapted to the needs of the company. The project features an optimized, cost-effective, and accurate approach to strengthening enterprise security and optimizing overall network performance.

Keywords : Firewall, Network Security, FortiGate, DMZ, IPS,WAF,Authorization, Traffic, Attacks

Introduction génerale

De nos jours, les attaques contre les réseaux informatique se multiplient, avec une sophistication croissante, une puissance accrue et une intelligence plus développée, engendrant des dommages considérables.Pour cela les organisations sont confrontées à un défi constant pour protéger leurs réseaux notamment les données sensibles et les systémes d'information en générale.De plus la protection des données sensibles est devenue une préoccupation majeure, notamment pour les organisations qui gèrent des informations sensibles et confidentielles. Cette évolution rapide a suscité l'intérêt des chercheurs et des professionnels pour comprendre les concepts de base de la sécurité informatique, les mécanismes de sécurité, ainsi que les méthodes et les outils de la protection.

L'objectif principale dans ce mémoire est donc de renforcer la sécurité du réseau de la direction générale de NESDA à l'aide d'un pare-feu de nouvelle génération(Next Generation Firewall) notamment "FortiGate" qui est déja installé sur le réseau.Pour atteindre notre objectif et répondre aux besoins de l'institution, nous avons déployé et mis en place des solutions et les appliquer via le firewall "FortiGate" en créant des nouveaux réseaux , mis en œuvre des restrictions et des règles pour assurer leurs protection, limiter et sécuriser certains accés à distance ou localement.

Notre mémoire comporte trois chapitres :

Nous allons préluder par « Généralités sur les réseaux et sécurité informatique » où nous allons commencer par présenter l'organisme d'accueil, quelques notions de base sur les réseaux informatiques d'une part et définir la sécurité informatique par décrire quelques termes, méthodes de sécurité et chiffrement de données d'autre part.

Le deuxième chapitre concerne « Les solutions de la sécurité informatique», dans ce chapitre, nous allons explorer les principaux solutions et procédures de la sécurité, en mettant l'accent sur les types d'attaques les plus courantes,les politique , les dispositifs et les technologies de sécurité.

Le troisième chapitre est consacré à présenter la partie pratique de notre projet, intitulé «La Mise en place et simulation », nous allons présenter les étapes de l'implémentation de notre solution. Nous commençons par décrire la problématique et les solutions proposées, l'environnement de développement puis les étapes de l'implémentation de notre solution .

Nous terminons par une conclusion générale qui résume l'apport essentiel de notre travail.

Chapitre I : Généralités sur les réseaux et la sécurité informatique

I.1.Introduction

L'utilisation des technologies de l'information et de la communication est devenue indispensable dans la plupart des entreprises modernes. Les réseaux informatiques permettent aux équipements de communiquer entre eux et de partager des informations nécessaires au bon fonctionnement de ces entreprises.Un système d'information qui néglige la protection de ses données et de ses communications peut avoir des grands risques, ainsi que la société qui l'utilise. C'est la raison pour laquelle la sécurité informatique s'occupe de toute protection.

Ce chapitre vise à présenter les notions de base des réseaux informatiques et les concepts de base liés au la sécurité informatique. Ces notions formeront la base nécessaire à notre contribution.

I.2. Organisme d'accueil

L' Agence Nationale de Soutien et de Développement de l'Entreprenariat en anglais National Entrepreneurship Support And Development Agency **"NESDA** s'agit d'un organisme gouvernemental de nature particulière, doté de la personnalité juridique et de l'indépendance financière. Sous la tutelle du ministre plénipotentiaire chargé des petites entreprises en qualité de vice-Premier ministre, cette agence accompagne les porteurs de projets dans la création et le développement de petites entreprises productrices de biens et de services.

Joue un rôle clé dans l'intensification du tissu industriel des petites et moyennes entreprises, en contribuant à la création d'emplois et à l'absorption du chômage, ainsi qu'en cherchant à développer la sous-traitance externe et à augmenter les exportations

L'Agence est chargée de gérer le dispositif d'accompagnement à la création de Microentreprises par des jeunes âgés entre 18 et 55 ans.

NESDA dispose d'un réseau de 61 agences, implantées dans toutes les wilayas du pays, auxquelles sont rattachées 177 antennes.

L'organisme a connu plusieurs changements durant plus de vingt ans d'existence. Ces changements répondaient à la nécessité d'améliorer le dispositif en termes de niveau d'aides, des conditions d'éligibilité ou encore pour le rendre plus attractif et plus efficace.

Les derniers changements viennent consolider la nouvelle approche et la nouvelle stratégie adoptée par les pouvoir publics visant à créer des microentreprises pérennes dans un écosystème favorable et encouragent. Cela s'est conjugué notamment par l'adaptation des textes régissant le dispositif à cette nouvelle stratégie, par la signature de convention de partenariat avec les différents acteurs (ministères, organismes publics…), et par le renforcement de l'accompagnement et de la formation des porteurs de projets.

L'agence est placée depuis le 5 mai 2020 sous la tutelle du Ministre Délégué auprès du Premier Ministre chargé de la microentreprise, des start-ups et de l'économie de la connaissance.

I.2.1. Les Objectifs de l'établissement

L' Agence Nationale de Soutien et de Développement de l'Entreprenariat a pour mission de :

- Encourager la création et le développement d'activités de production des produits et des services par les porteurs de projets.
- Promouvoir toutes formes d'actions et de mesures visant à promouvoir l'esprit d'entreprise

I.2.2. Tâches de l'établissement

Les tâches de l' Agence Nationale de Soutien et de Développement de l'Entreprenariat comprennent:

- Soutenir et fournir des conseils et accompagner
- Fournir toutes les informations économiques, techniques, législatives et réglementaires liées aux activités des titulaires de projet.
- Développer les relations avec les partenaires et parties prenantes (banques, Autorité Fiscale, Caisse de Sécurité Sociale)
- Développer des partenariats entre différents secteurs pour identifier les opportunités d'investissement
- Former les porteurs de projets au sein des centres de développement de l'entrepreneuriat
- Financer des projets jeunes et les informer sur les différentes subventions accordées. .
- Accompagnement et suivi à distance Pour les petites entreprises créées par des entrepreneurs

Nesda assure une formation sur la technique de gestion de la micro-entreprise au profit des porteurs de projets. Ces formations constituent une étape primordiale car indispensable au passage à l'étape du projet financier.

I.2.3.Organigramme de l'organisme d'accueil

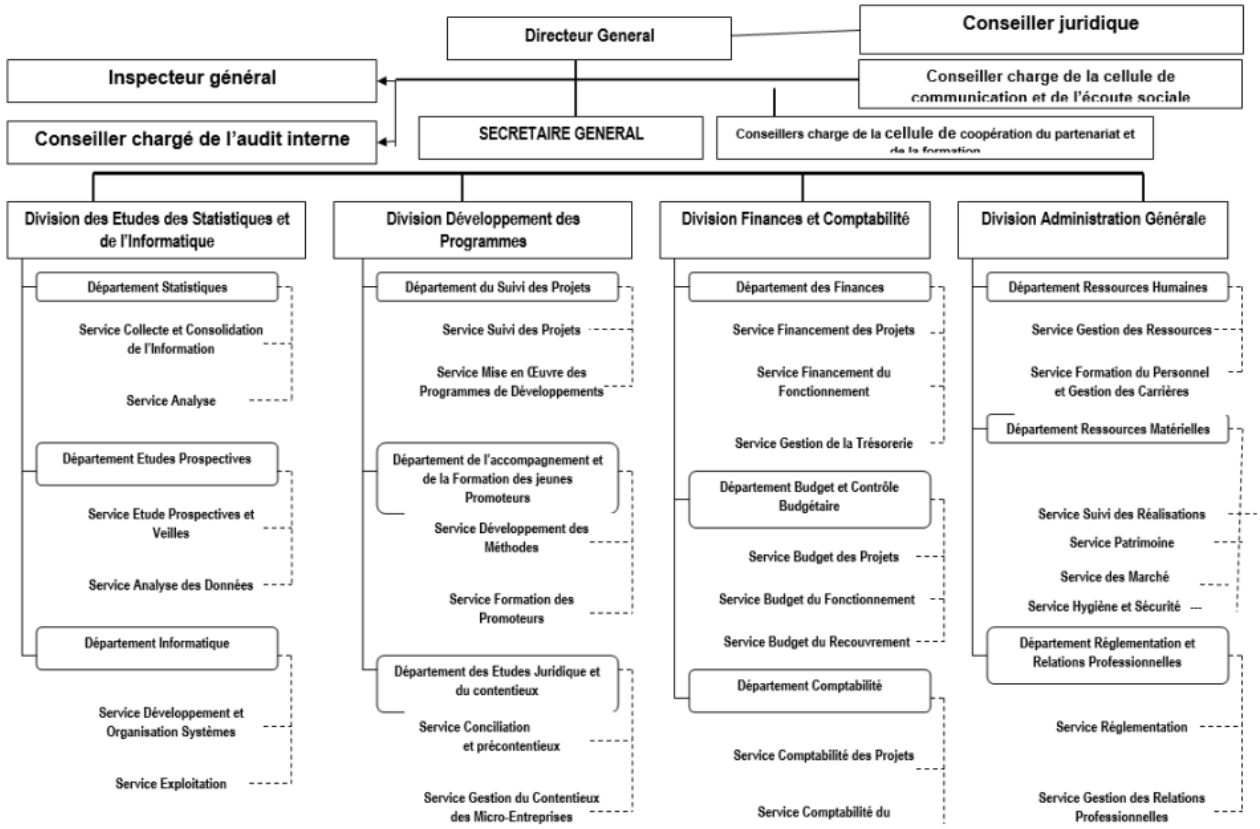

Figure I-1::Organigramme de Nesda

I.3. Conceptes et notions sur les réseaux informatique

I.3.1. Définition d'un réseau informatique

C'est l'ensemble d'ordinateurs (ou de périphériques) autonomes connectés entre eux et qui sont situés dans un certain domaine géographique.Deux stations sont considérés comme interconnectées si elles sont capables d'échanger de l'information. [1]

I.3.2.Les Besoins des Réseaux

Les réseaux sont bien évidement nés d'un besoin d'échanger de l'information entre les machines.Ainsi une entreprise possédant plusieurs lieux peut avoir un ordinateur sur chaque site pour, par exemple gérer le stocke,paye,production..ct.Cependant,le besoin de communication va inciter le management à connecter ces ordinateurs pour pouvoire extraire et échanger des informations concernant tout l'entreprise. [1]

I.3.3.Avantages d'un Réseau

Un réseau permet :

- Le partage e fichiers : les données circule par un câble et non par des support amovibles(clefs usb,disquette)

- Tous les ordinateurs du réseau peuvent accéder aux mêmes données et les modifier
- Le partage de ressources matérielles : imprimante,cédérom ;modem,disque dur…
- Le partage des applications :travail dans un environnement Multi-Utilisateurs.
- La garantie de l'unicité de l'information (base de données)
- La communication entre personnes (courrier électroique,discussion en direct,..)[w1]

I.3.4.Architectures des Réseaux

I.3.4.1. Architecture Poste à Poste

Le poste à poste (en anglais, P2P) est un autre type d'architecture réseau où chaque ordinateur ou logiciel joue le rôle de client et de serveur. Cette structure n'est adaptée qu'à un réseau de petite taille.[W2]

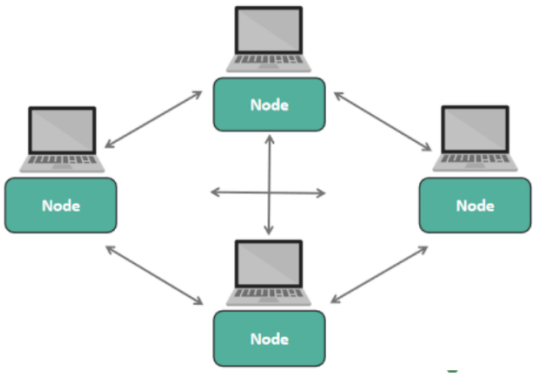

Figure I-2: Architecture poste à poste[W27]

I.3.4.2. Architecture Trois tiers

Dans les structures à trois niveaux (connues sous le nom d'architecture 3-tier), il y a un niveau intermédiaire, c'est-à-dire qu'il y a généralement une architecture partagée entre :

- Le client est le demandeur de ressources.
- Le serveur d'application assure la fourniture de la ressource en utilisant un autre serveur.
- Le serveur secondaire(serveur de base de données), fournissant un service au premier serveur.[1]

Figure I-3:Architecture trois tiers[W28]

I.3.4.3. Architecture Client/Serveur

L'architecture client/serveur fait référence à un système de communication entre différents ordinateurs d'un réseau qui différencie un ou plusieurs clients d'un serveur : chaque logiciel client a la capacité d'envoyer des demandes à un serveur. Il est possible d'avoir un serveur spécialisé dans les domaines des applications, des fichiers ou de la messagerie électronique. Les postes de travail ne nécessitent qu'un petit fichier logiciel (connu sous le nom de client) pour se connecter au serveur, peu importe le système d'exploitation installé sur ces postes.[W2]

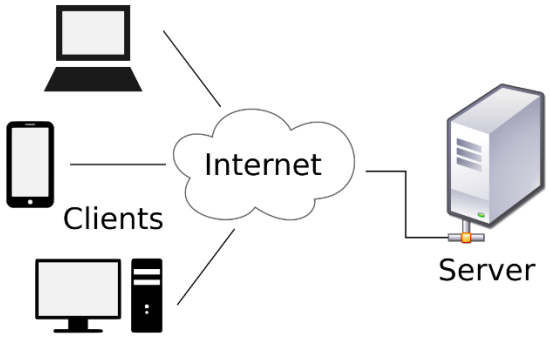

Figure I-4:Architecture Client/serveur[W29]

I.3.5.Les Serveurs

Dans les réseaux informatiques, un serveur est à la fois un logiciel et l'ordinateur qui le stocke. Son rôle est de répondre automatiquement aux requêtes envoyées par clients (ordinateurs et logiciels) sur le réseau.

I.3.5.1.Le Serveur Dhcp

Le protocole DHCP (Dynamic Host Configuration Protocol) est un protocole réseau client/serveur standardisé qui attribue dynamiquement des adresses IP et d'autres informations de configuration aux périphériques réseau. Chaque périphérique d'un réseau TCP/IP doit disposer d'une adresse IP unicast unique pour accéder au réseau et à ses ressources. Sans DHCP, les adresses IP des nouveaux ordinateurs ou des ordinateurs qui ont été retirés d'un sous-réseau à un autre doivent être configurées manuellement. [3]

Il fournit une façon automatisée de distribuer et mise à jour des adresses d'IP et d'autre informations de configuration(ex:default gateway) sur un réseau.

Un serveur DHCP fournit ces informations à un client DHCP par l'échange d'une série de messages, connus par la conversation DHCP ou la transaction DHCP. Si le le serveur DHCP et les clients DHCP sont trouvés sur différents sous-réseaux, un agent de relais DHCP est utilisé pour faciliter la conversation. [3]

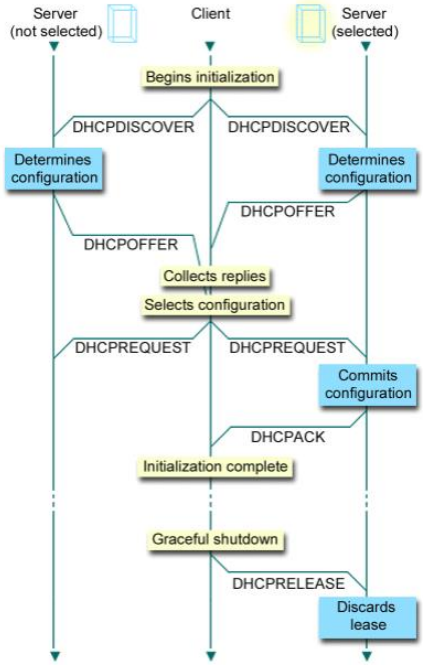

Figure I-5: Les Opération de Serveur Dhcp[W30]

I.3.5.2.Le Serveur Dns

Le système de noms de domaine (DNS) est un système de base de données distribué pour gérer les noms d'hôte et leurs adresses IP (Internet Protocol) associées. [2]

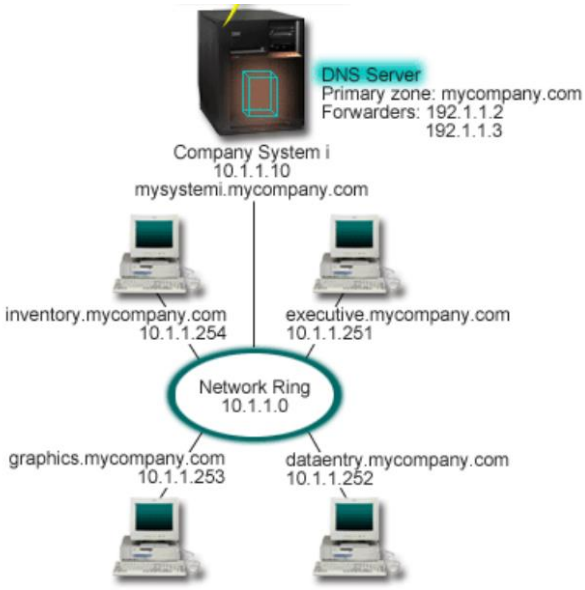

Figure I-6: Un Serveur Dns[4]

Les informations DNS sont réparties en une structure de domaines. Il incombe aux serveurs de ne connaître qu'une faible partie des données, tel un sous-domaine unique. La zone est la partie d'un domaine dont le serveur est directement responsable. Un serveur DNS qui possède toutes les informations et données sur l'hôte d'une zone exerce une autorité sur la zone. L'autorité d'un serveur permet de répondre aux demandes concernant les hôtes de sa zone en utilisant ses

propres enregistrements de ressources. Le processus de demande est influencé par plusieurs éléments. La compréhension des demandes DNS expose les différentes approches qu'un client peut adopter pour résoudre une demande. [4]

I.3.5.3.Serveur Web

Un serveur Web est un ordinateur qui stocke le logiciel du serveur Web et les fichiers de composants d'un site Web (par exemple, des documents HTML, des images, des feuilles de style CSS et des fichiers JavaScript). Un serveur Web se connecte à Internet et prend en charge l'échange de données physiques avec d'autres appareils connectés au Web. [W4]

Côté logiciel, un serveur web comprend plusieurs parties qui contrôlent la façon dont les uilisateurs accèdent aux fichiers hébergés. Au minimum, il s'agit d'un serveur HTTP. Un serveur HTTP est un logiciel qui comprend les URL (adresses Web) et HTTP (le protocole que votre navigateur utilise pour afficher les pages Web). Un serveur HTTP (apache,nginix) est accessible via les noms de domaine des sites Web qu'il stocke, et il fournit le contenu de ces sites Web hébergés à l'appareil de l'utilisateur final.

Au niveau le plus élémentaire, chaque fois qu'un navigateur (firefox,chrome) a besoin d'un fichier hébergé sur un serveur Web, le navigateur demande le fichier via HTTP. Lorsque la requête atteint le bon serveur web (matériel), le serveur HTTP (logiciel) accepte la demande, trouve le document demandé et le renvoie au navigateur, également via HTTP. (Si le serveur ne trouve pas le document demandé, il renvoie une réponse 404 à la place.) [W4]

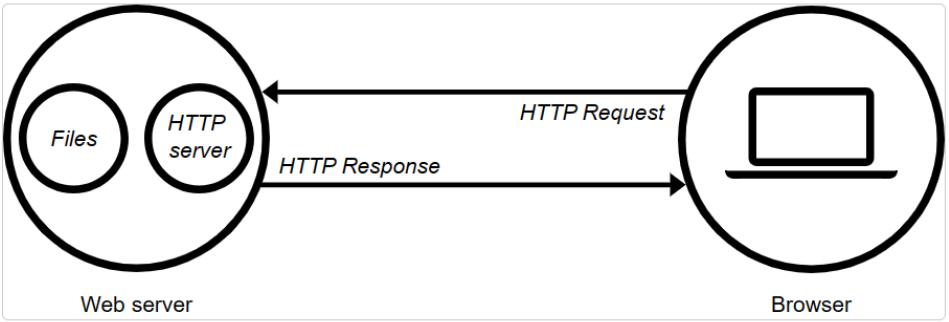

Figure I-7: L'interaction de Client avec le serveur Web[W4]

I.3.5.4.Serveur de Fichiers

Un serveur de fichiers est un ordinateur chargé de conserver et de gérer les fichiers de données pour permettre à d'autres ordinateurs du même réseau d'accéder aux fichiers. Il offre aux utilisateurs la possibilité de partager des données sur un réseau sans nécessiter de transfert physique de fichiers. Le serveur de fichiers est un ordinateur ou un serveur qui permet de stocker et de mettre à disposition des objets BLOB de données aux clients, servant ainsi de point central pour le stockage et le partage de fichiers au sein d'un réseau. Ils peuvent être restreints à un réseau local unique (LAN) ou être connectés à Internet. [W3]

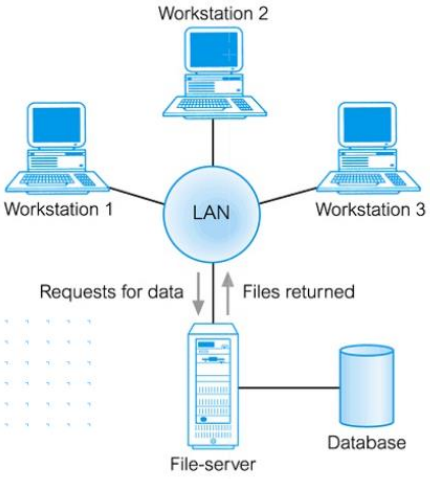

Figure I-8: Le Serveur des Fichiers[W31]

Les serveurs de fichiers ne permettent d'accéder aux clients qu'à un système de fichiers distant. Tous les types de données peuvent être stockés par eux, tels que des exécutables, des documents, des photos ou des vidéos. En général, ils conservent les données en utilisant des objets de données en bloc ou des fichiers binaires. Ils ne procèdent pas à une indexation ou à un traitement supplémentaire des fichiers qui y sont stockés. Il est possible que des plugins ou des fonctions de serveur supplémentaires soient disponibles, offrant ainsi des fonctionnalités supplémentaires. [W3]

I.3.6. Contrôleur de Domaine(Domain Controller)

Un contrôleur de domaine (DC) est un serveur spécial qui fournit des services critiques tels que l'authentification et l'autorisation pour un domaine Active Directory. Plus précisément, un contrôleur de domaine est un ordinateur qui exécute le système d'exploitation Windows Server et sur lequel Active Directory Domain Services (AD DS) est installé. Les ordinateurs de bureau, les ordinateurs portables et les autres machines exécutant une version normale de Windows ne peuvent pas être des contrôleurs de domaine[W5]

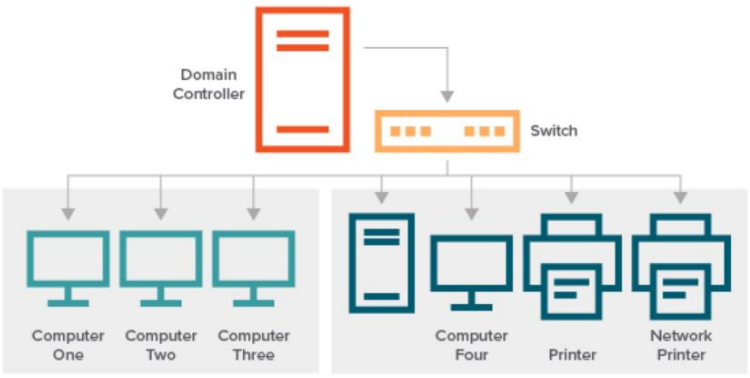

Figure I-9: Controleur de Domaine dans un Réseau lan[W5]

Chaque contrôleur de domaine d'un domaine stocke une copie de répertoire et fournit des services AD tels que l'authentification et l'autorisation. Le fichier de répertoire, Ntds.dit, contient des détails sur les utilisateurs, les ordinateurs, les groupes de sécurité et d'autres objets de ce domaine. Il inclut également des informations sur le schéma Active Directory, qui définit toutes les classes d'objets qui peuvent être stockées dans le répertoire. Les modifications apportées à la copie de répertoire d'un contrôleur de domaine (par exemple, lorsqu'un utilisateur modifie son mot de passe ou qu'un compte d'utilisateur est verrouillé en raison d'un trop grand nombre de mots de passe incorrects) sont répliquées sur les autres contrôleurs de domaine du domaine afin qu'ils restent tous à jour. [W5]

I.3.6.1.Active Direcotry Domain services (AD DS)

Le service de répertoire Active Directory est intégré sur Windows Server. Active Directory comprend le dossier qui conserve les données sur vos ressources distribuées, ainsi que les services qui facilitent la disponibilité et l'utilisation des informations. Tous les systèmes d'exploitation Windows Server actuels supportent Active Directory.

La gestion centralisée des ressources réseau est possible grâce à Active Directory, un service extensible. Il facilite l'ajout, la suppression ou le transfert de comptes pour les utilisateurs, les groupes et les ordinateurs, ainsi que d'autres types de ressources. La plupart des tâches administratives que vous réalisez ont un impact sur Active Directory de manière ou d'autre. Active Directory repose sur les protocoles Internet courants et possède une conception qui facilite l'identification des éléments physiques et logiques de la structure de votre réseau de manière claire.[5]

I.3.6.2. Services de AD

Active Directory offre les ressources requises pour concevoir un répertoire adapté aux exigences de votre entreprise. Un répertoire est une base de données regroupant des informations sur diverses ressources. Dans un système informatique distribué comme un réseau Windows, il est essentiel que les utilisateurs puissent localiser et utiliser des ressources distribuées, tandis que les administrateurs doivent être capables de gérer l'utilisation des ressources distribuées. C'est la raison pour laquelle un service de répertoire est essentiel.

Toutes les informations requises pour l'utilisation et la gestion des ressources distribuées sont stockées dans un emplacement centralisé dans un AD DS. Le service offre la possibilité aux ressources de collaborer. Il a pour mission d'autoriser l'accès, de gérer les identités et de superviser les interactions entre les ressources. Comme un service de répertoire assure ces fonctions essentielles, il est nécessaire qu'il soit étroitement lié aux fonctions de sécurité et de gestion du système d'exploitation réseau.[5]

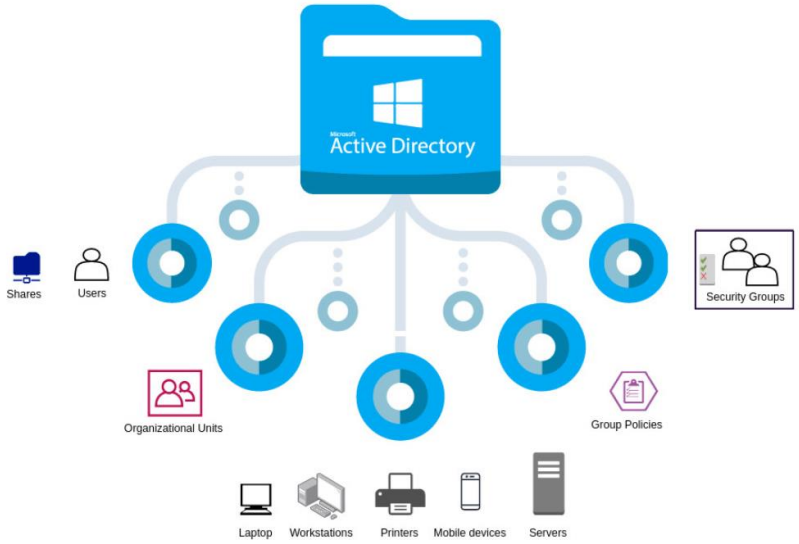

Figure I-10: Les Services de AD DS[W32]

Des listes de contrôle d'accès (ACL) sont également stockées avec chaque ressource, ce qui vous permet de conserver les permissions permettant aux personnes d'accéder au ressource et de le gérer. Le fait de disposer d'une source unique pour ces informations les rend plus accessibles et plus faciles à gérer[6]

- **Active Directory Replication**

Dans la majorité des répertoires, les données d'un seul serveur maître sont réparties vers des serveurs dédiés. C'est la manière dont la réplication fonctionne.évidemment ,il est clair qu'il y a plusieurs problèmes potentiels liés à un schéma de réplication à maître unique, tels que le point de défaillance unique des mises à jour, la distance géographique entre le maître et les clients lors de l'exécution des mises à jour, ainsi qu'une réplication moins efficace en raison du fait que les mises à jour ont un seul point d'origine. Ces problèmes sont résolus grâce à la réplication Active Directory, afin de profiter de la réplication multimaître vous devez d'abord créer une topologie de site qui décrit le réseau et aide à définir la manière dont les contrôleurs de domaine doivent se répliquer les uns avec les autres.[6]

- **Active Directory Sites et Subnets**

Les sites et les sous-réseaux (Subnets) sont les composants physiques d'Active Directory(le côté physique d'Active Directory). L'objectif principal d'un site est de regrouper physiquement les ordinateurs afin d'optimiser le trafic d'ouverture de session, d'authentification et de réplication. Les sites facilitent l'ouverture de session(logon) et l'authentification en déterminant le contrôleur de domaine le plus proche en fonction de l'emplacement du site lorsqu'un

utilisateur se connecte. Les sites facilitent la réplication en limitant le trafic de réplication aux périphériques d'un site, et en fournissant des mécanismes pour contrôler la réplication entre les sites.[5]

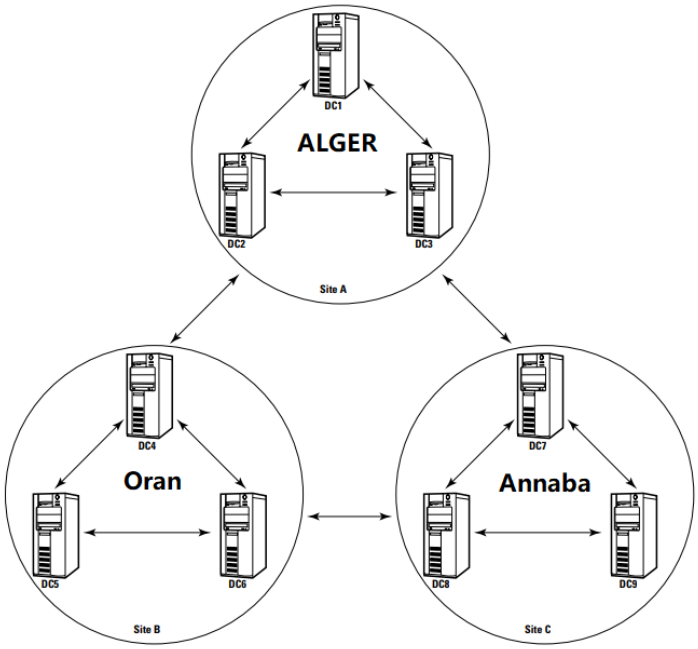

Figure I-11: Active Directory Replication interSites[7]

Les Ordinateurs clients AD (ordinateurs de bureau/portables et non -Les serveurs DC), en revanche, sont associés dynamiquement à un site au moment du démarrage(boot). Le contrôleur de domaine, dans le cadre du processus de démarrage du client, compare le sous-réseau IP du client avec les définitions du site AD et détermine de quel site le client est membre. Dans la mesure du possible, les ordinateurs clients AD tentent toujours d'obtenir leurs services AD à partir de contrôleurs de domaine(DC) qui se trouvent sur le même site avant de les rechercher dans d'autres sites. De cette façon, les requêtes AD sont localisées dans le site autant que possible.[7]

Les sous-réseaux (Subnets) sont décrits par leurs adresses réseau IP combinées à un masque de sous-réseau mesuré en bits (ex :10.10.1.0/24). Les objets de sous-réseau(subnets) dans Active Directory sont une représentation logique des sous-réseaux de votre environnement (physique). Lorsque vous déployez Active Directory, il est nécessaire de créer des objets de sous-réseau pour chaque sous-réseau TCP/IP dans lequel tous les contrôleurs de domaine AD seront installés et où se trouvent les objets de sous-réseau de tous les clients d'Active Directory. Ces objets de sous-réseau sont ensuite associés à l'objet site. Un objet de sous-réseau ne peut être associé qu'à un seul site dans Active Directory. L'association de sous-réseaux à un site

permet aux contrôleurs de domaine et au client AD de déterminer le site dans lequel ils se trouvent.[7]

- **AD Sites Links**

Il est important d'avoir des sites, mais il est essentiel de pouvoir les connecter si vous souhaitez un jour répliquer des données. Une telle connexion entre sites est appelée lien de site (site link). L'administrateur crée manuellement des liens de site afin de signaler la possibilité pour deux sites ou plus de se répliquer l'un avec l'autre. Si le réseau physique sous-jacent est déjà connecté à plusieurs sites, les liens de site peuvent établir une connexion entre plusieurs sites. Toutefois, les connexions de réplication sont souvent plus faciles à visualiser et à contrôler si vous vous restreignez à deux sites par lien de site.[6]

Par défaut, les liens de site créent une connectivité transitive entre les sites. Si nous créons un lien de site entre les sites A et B et un autre lien de site entre les sites B et C, une connexion automatique (appelée pont de lien de site) est créée entre les sites A et C, comme illustré à la figure.[7]

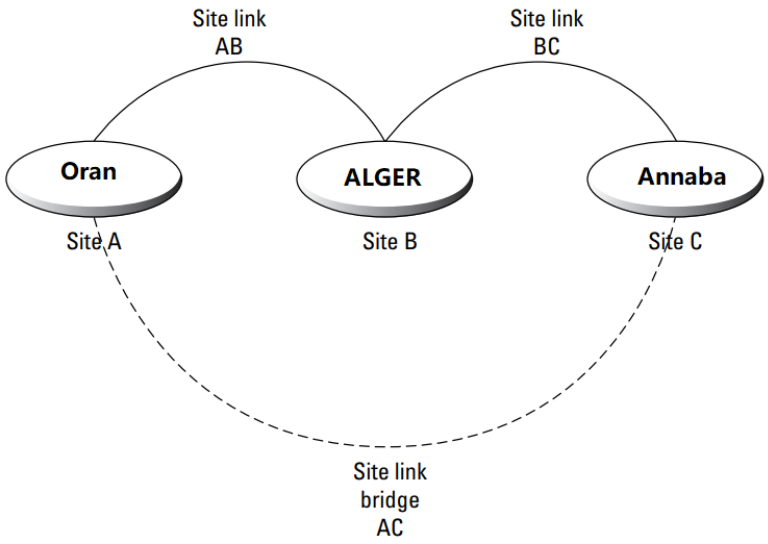

Figure I-12:Représentation de liens de sites dans AD[7]

I.4. Concepts et notions sur la Sécurité informatique

La mise en place de la cybersécurité ne nécessite pas un coût considérable ou une période de transition très courte. Peu importe la taille de l'entreprise, l'amélioration de la sécurité informatique assure la protection de vos données et de celles de vos clients, améliore les relations commerciales.[8]

I.4.1.Classification des menaces de sécurité

- Une Menace physique : Les attaques physiques contre les systèmes et les cadres informatiques peuvent prendre de nombreuses formes, notamment la destruction de

l'ensemble de l'infrastructure réseau, les dommages aux machines, les dommages aux logiciels et à la programmation informatiques, le vol de matériel informatique, le vandalisme et les catastrophes naturelles telles que les inondations, les incendies, les tremblements de terre et les guerres. [9]

- Une Erreur accidentelle : un enjeu de sécurité majeur que les experts en sécurité informatique doivent toujours tenir compte lorsqu'ils organisent les mesures de sécurité d'un système. Il est possible que des erreurs involontaires ou accidentelles se produisent dans un système informatique, mais il est primordial que le concepteur prenne en compte la mise en œuvre de contrôles légitimes. La dégradation de l'information causée par une erreur de programmation, une erreur du client ou de l'administrateur est considérée comme une erreur accidentelle. [9]
- Un Accès non autorisé : Pour que les données soient transformées en informations utiles, il faut que les informations stockées sur le système informatique soient accessibles. En raison de l'accès du système par des utilisateurs non autorisés, cela pose également un risque de sécurité inhabituel pour le système informatique. De plus, tout au long du processus de transfert de données entre les sites via un support réseau, qui comprend à la fois des supports filaires et sans fil, l'accès aux données peut être facilité par un système distant. [9]
- Malware: Tout type d'altération du système informatique qui incorpore la pénétration, les chevaux de Troie, les virus et tout type de modification illicite du système informatique qui incorpore en outre la génération de codes illégaux pour modifier les codes standard à l'intérieur du système peut être qualifié d'utilisation abusive malveillante. Cela pourrait également provoquer un malheur ou des pertes incroyables liés à l'argent et devrait être évité dans tous les cas. De manière générale, il existe deux catégories de logiciels malveillants , Méthodes d'infection comme les virus,trojan et worms et la deuxiéme est les Actions des logiciels malveillants comme spyware,ransomware et rootkite.[9]

I.4.2.La Sécurité de l'information

La sécurité de l'information vise à assurer la confidentialité, l'intégrité et la disponibilité (C, I et A [availability]) de toutes les informations détenues par une organisation, qu'elles soient électroniques ou sur papier. Par conséquent, la sécurité de l'information implique généralement de prendre en compte les contrôles physiques et environnementaux en plus des contrôles technologiques.[8]

Figure I-13:Le triangle CIA[W33]

- La Confidentialité – est la garantie que des données, des services ou tout autre bien ne sont accessibles qu'aux personnes autorisées. La confidentialité est compromise dès lors qu'une personne non autorisée accède à des données ou tout autre bien sans en avoir le droit. Par exemple, si une personne parvient à ouvrir un téléphone mobile et à accéder aux informations contenues dedans.
- L'Intégrité - est la propriété garantissant que des données sont exactes, complètes et n'ont pas été modifiées. L'intégrité peut être compromise par la modification du contenu d'un fichier. Par exemple, l'intégrité des notes d'élèves sur un espace numérique de travail est compromise si ses notes sont modifiées par une personne n'ayant pas le droit de le faire.
- La Disponibilité –est la capacité à accéder à des données ou à un service au moment souhaité. Elle peut être, par exemple, compromise par la destruction (effacement de données), le chiffrement (les informations deviennent illisibles à moins de posséder la clé de déchiffrement) ou encore par l'interruption d'un service. Un ordinateur peut devenir inaccessible si un logiciel malveillant chiffre l'ensemble des données qu'il contient.[10]

I.4.3.La Cybersécurité

La cybersécurité englobe de manière schématique deux aspects principaux.

1. **La prévention :** correspond à l'ensemble des mesures permettant de renforcer la sécurité d'un système d'information pour lui permettre de résister aux attaques susceptibles de menacer les données et les services auxquels il permet d'accéder.
   La prévention passe principalement par : [10]

- La mise en place de mesures de sécurité adaptées notamment au niveau technique, comme le fait de sauvegarder régulièrement les données dans un environnement distinct et sécurisé ou encore de chiffrer de bout-en-bout des conversations via une messagerie.
- La sensibilisation des personnes aux risques et aux bonnes pratiques de sécurité informatique pour éviter que des erreurs ou des négligences facilitent le travail des attaquants, par exemple, en affichant son code PIN au dos de son téléphone.
- Pour aller plus loin, l'analyse approfondie des risques pour un système d'information ou pour une organisation permettant d'identifier des mesures de sécurité complémentaires renforçant leur sécurité. [10]

2. **La réaction :** correspond à l'ensemble des moyens et des activités permettant de détecter et de répondre aux cyberattaques en vue de les stopper et de revenir à un mode de fonctionnement normal.La réponse aux cyberattaques implique principalement :

- la Détection des attaques informatiques.
- La prise en charge d'un incident, en mobilisant des équipes techniques (les CSIRT).
- La prise en charge d'une crise cyber au sein d'une entreprise.
- La reconstruction des systèmes d'information infectés
- La lutte contre les criminels en ligne [10]

I.4.4.L'importance de la Cybersécurité

La cybersécurité est une fonction fondamentale et une sauvegarde nécessaire pour de nombreuses organisations en raison de la forte dépendance à l'égard des ordinateurs dans une industrie de pointe qui stocke et transmet une pléthore de données sensibles et personnelles sur les individus.

À mesure que le volume des cyberattaques augmente, les organisations et les associations, en particulier celles qui traitent des informations et des données relatives à la sécurité nationale, à la santé ou aux dossiers monétaires, doivent trouver un moyen de garantir leurs données commerciales et individuelles délicates.[9]

I.4.5.Termes de Sécurité

- **Actifs :** Un actif est tout ce qui a de la valeur pour l'organisation. Cela comprend les personnes, les équipements, les ressources et les données. [13]
- **Menace :** Une menace est un danger potentiel pour les actifs, les données ou les fonctionnalités du réseau d'une entreprise. [13]
- **Exploiter :** Un exploit est un mécanisme qui profite d'une vulnérabilité

- **Atténuation :** L'atténuation est la contre-mesure qui réduit la probabilité ou la gravité d'une menace ou d'un risque potentiel. La sécurité du réseau implique plusieurs techniques d'atténuation. [13]
- **Risque :** Le risque est la probabilité qu'une menace exploite la vulnérabilité d'un actif, dans le but d'affecter négativement une organisation. Le risque est mesuré à l'aide de la probabilité de survenance d'un événement et de ses conséquences.[13]
- **Les vulnérabilités :**Une vulnérabilité est une faiblesse d'un système, ou de sa conception, qui pourrait être exploitée par une menace[13]. Les vulnérabilités peuvent être de différentes natures ;Une vulnérabilité au sein d'un équipement ou du code d'un logiciel, présente par négligence ou introduite dès la conception de manière involontaire. [10]

I.4.6.Les Méthodes de sécurité de données

La Confidantialité, Un cadre sécurisé garantit la confidentialité des informations. Cela signifie que cela permet aux individus de voir uniquement les informations qu'ils devraient voir. La sécurité a plusieurs points de vue tels que la protection des correspondances, la sécurité des informations importantes, la vérification des clients et l'approbation des clients. [9]

La Confidentialité des communications, La diffusion de données personnelles privées, telles que les dossiers de crédit, médicaux et commerciaux, doit être contenue par le SGBD. De plus, il devait garder les informations de l'entreprise en sécurité et hors de portée des personnes non autorisées. Il peut s'agir, par exemple, d'informations privilégiées échangées, d'informations confidentielles sur les produits et les processus, d'enquêtes sérieuses et de plans de marketing et de vente. [9]

L'authentification, L'une des idées les plus fondamentales en matière de sécurité des bases de données est la validation, qui est essentiellement la procédure par laquelle le cadre informatique vérifie l'identité d'un client, Un client peut réagir à une sollicitation de vérification en donnant une preuve d'identité ou un jeton de confirmation. Par exemple : Si vous avez déjà présenté une pièce d'identité avec photo (par exemple, lors de l'ouverture d'un compte), vous avez reçu une demande d'authentification. Vous avez démontré votre identité en indiquant votre permis de conduire (ou une autre pièce d'identité). Dans ce cas, votre permis de conduire a été rempli en guise de jeton de confirmation. [9]

L'autorisation, Un client validé fait l'expérience du deuxième niveau de sécurité, l'autorisation. Il s'agit de la procédure par laquelle le framework collecte des informations sur le client vérifié,

y compris les opérations de base de données que le client peut effectuer et les objets de données auxquels il peut accéder. [9]

I.4.7. Chiffrement des données(Data Encryption)

La perte d'un nombre suffisant de données, surtout si elle est due à l'incompétence, pourrait être un business-ending event . Le chiffrement fournit une couche sécurisée.Le chiffrement des données empêche les données d'être exposées à un accès non autorisé et les rend inutilisables. La détection nous permet de surveiller les activités des utilisateurs du réseau et fournit un moyen de différencier les niveaux d'activités et offre un indice possible sur les violations du réseau.[12]

La cryptographie, un mot dont les causes sont grecques, signifie « écriture secrète ». Cependant, nous utilisons le terme pour faire allusion à la science et à l'art de changer les messages pour les rendre sûrs et invulnérables aux agressions. La figure I.14 montre les parties associées à la cryptographie. [9]

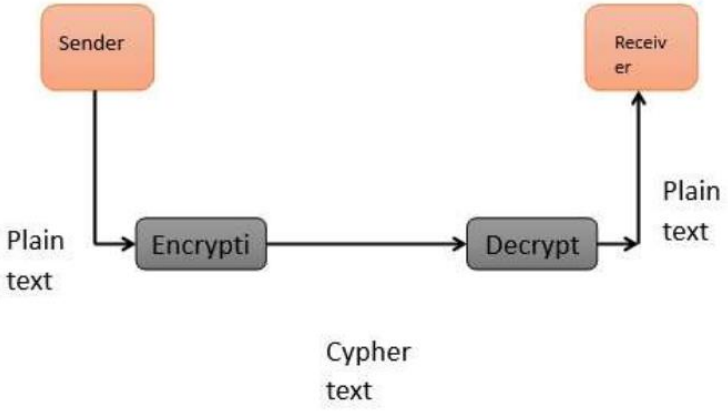

Figure I-14:Le proccesus de la cryptographie[9]

Un message unique est connu sous le nom de texte en clair(plaintext), tandis que le message codé est connu sous le nom de texte chiffré(ciphertext). .Les données, ou « texte en clair » ,sont traduites en texte chiffré par un processus de chiffrement(ciphering process).

Le moyen de passer du texte en clair au texte chiffré est connu sous le nom de chiffrement(encryption) ; Rétablir le texte en clair à partir du texte chiffré est l'interprétation ou le déchiffrement(decryption).[9]

I.5. Les Réseaux DMZ

Une zone démilitarisée, également connue sous le nom de DMZ, est un réseau périmétrique qui garantit la protection et l'ajout d'une couche de sécurité supplémentaire au réseau interne d'une organisation contre le trafic irrégulier.

Le but ultime d'un réseau de zone démilitarisé est de donner à une organisation la possibilité d'accéder à des réseaux non fiables, comme Internet, tout en garantissant la sécurité de son réseau privé ou de son réseau local. La DMZ est généralement utilisée par les organisations pour stocker des services et des ressources externes, ainsi que des serveurs pour le système de noms de domaine (DNS), le protocole de transfert de fichiers (FTP), la messagerie, le proxy, le protocole VoIP (Voice over Internet Protocol) et les serveurs Web. [W6]

Ces serveurs et ressources sont séparés et ont un accès restreint au réseau local (LAN) pour garantir leur accessibilité via Internet, mais pas via le réseau local interne. Il est donc plus compliqué pour un hacker d'accéder directement aux données et aux serveurs internes d'une organisation grâce à une approche DMZ. Les vulnérabilités de son réseau local peuvent être réduites par une entreprise, ce qui crée un environnement sécurisé contre les menaces tout en assurant que les employés peuvent communiquer de manière efficace et partager des informations directement via une connexion sécurisée.[W6]

I.5.1.Les Avantages de l'utilisation d'une DMZ

Le principal bénéfice d'une DMZ réside dans sa capacité à offrir à un réseau interne une couche de sécurité avancée en restreignant l'accès aux informations confidentielles. Les visiteurs du site web peuvent bénéficier de certains services grâce à une DMZ qui sert de connexion entre eux et le réseau privé de l'entreprise. Ainsi, la DMZ présente également d'autres bénéfices en termes de sécurité, [W6] tels que :

- Afin de simplifier le contrôle d'accès, les entreprises ont la possibilité de permettre aux utilisateurs d'accéder à des services en dehors de leur réseau grâce à l'Internet public. La DMZ facilite l'accès à ces services tout en appliquant la segmentation du réseau afin de rendre plus compliqué pour un utilisateur non autorisé d'accéder au réseau privé. Un serveur proxy peut aussi être inclus dans une DMZ, ce qui permet de regrouper le flux de trafic interne et de faciliter la surveillance et l'enregistrement de ce trafic.
- Prévention de la reconnaissance du réseau : Une DMZ permet aux attaquants de ne pas pouvoir effectuer le travail de reconnaissance qu'ils effectuent à la recherche de cibles potentielles en fournissant un tampon entre Internet et un réseau privé. Les serveurs de la DMZ sont accessibles au public, mais sont protégés par un pare-feu qui empêche

toute intrusion dans le réseau interne. En cas de compromission d'un système DMZ, le pare-feu interne sépare le réseau privé de la DMZ afin de garantir sa sécurité et de compliquer la reconnaissance externe.

- Bloquer l'usurpation de protocole Internet (IP) : Les cybercriminels cherchent à accéder aux systèmes en utilisant une adresse IP falsifiée et en faisant l'identité d'un appareil autorisé connecté à un réseau. De telles tentatives d'usurpation d'identité peuvent être détectées et bloquées par une DMZ, car un autre service vérifie la validité de l'adresse IP. L'utilisation de la DMZ permet aussi de diviser le réseau pour créer un espace où le trafic peut être structuré et où les services publics peuvent être accessibles en dehors du réseau privé interne.[W6]

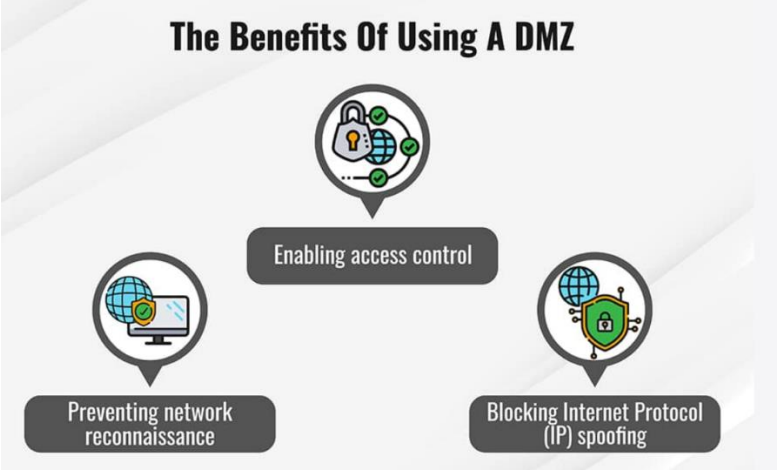

Figure I-15:les avantages de DMZ[W6]

Les services d'une DMZ comprennent :

- Les serveurs DNS
- Les serveurs FTP
- Les serveurs de messagerie
- Les serveurs proxy
- Les serveurs Web

I.5.2.Conception et architecture DMZ

Une DMZ est un « réseau ouvert », mais elle peut être protégée de différentes manières, d'une approche à pare-feu unique à des pare-feux doubles et multiples, la plupart des architectures DMZ modernes utilisent des pare-feux doubles qui peuvent être étendues pour développer des systèmes plus complexes. [W6]

1. **Pare-feu unique :** Une DMZ avec une configuration à pare-feu unique requiert au moins trois interfaces réseau. Le réseau externe, qui permet de connecter la connexion Internet publique au pare-feu, est le premier. Le réseau interne est le deuxième et le troisième est connecté à la DMZ. Différentes réglementations assurent la surveillance et le contrôle du trafic autorisé à accéder à la DMZ, tout en restreignant la capacité de connexion au réseau interne.
2. **Double pare-feu :** L'installation de deux pare-feux avec une DMZ entre eux est généralement une solution plus sécurisée, le premier pare-feu ne permettant que le trafic externe vers la DMZ et le second pare-feu ne permettant que le trafic qui relie la DMZ au réseau interne, un attaquant devant compromettre les deux pare-feux pour accéder au réseau LAN de l'entreprise.[W6]

I.6.Conclusion

Dans ce chapitre nous avons fait une étude génerale sur les réseaux informatiques, en couvrant les différents aspects tels que la définition et les avantages des réseaux ,les architectures,des éxplication sur les différents serveur et une présentations des services de AD DS.

Puis nous avons passé au sécurité informatique, en méttant l'accent sur la sécurité de l'information ,les classifications et les types des menaces,les vulnérabilités plus des notion sur la cybersécurité et le chiffrement des données en finirons par les réseaux DMZ.

Chapitre II :Les Solutions de La Sécurité Informatique

II.1.Introduction

Dans le Domaine de la sécurité des réseaux informatique, le premier major comme un responsable sur la sécurité reseau de l'entreprise est bien évidemment connaître et comprendre les différents solutions de la sècuritè informatique,afin de s'assurer la protection de votre réseau. Dans ce chapitre, nous allons explorer les principaux aspects de ses solutions, en mettant l'accent tout d'abord sur les différents menaces, attaques informatique ,les politiques de sécurité et comment gérer les risques.Puis, nous avons présenté les dispositifs de sécurité avec les technologies integrées dedans.

II.2.Les Types des Attaques

Tandis que les technologies évoluent, les cybercriminels redoublent d'inventivité pour accéder aux systèmes et aux données des entreprises. En 2023, la plateforme cybermalveillance.gouv recense 51 types d'attaques informatiques différents. Ce chiffre impressionnant met en exergue la pression qui pèse sur les infrastructures informatiques. Ces dernières années, les cyberattaques se font plus nombreuses mais aussi plus variées. Connaître les spécificités de chaque type d'attaque informatique est un enjeu de cybersécurité essentiel.

II.2.1.Attaque par écoute(eavesdropping)

C'est le moment ou un acteur malveillant capture et « écoute » le trafic réseau. Cette attaque est également appelée sniffing ou snooping. Afin d'approfondir la définition de « attaque par écoute », en général, il se produit lorsque quelqu'un se connecte à un réseau où le trafic n'est pas sécurisé ou chiffré et envoie des informations commerciales sensibles à un collègue. Les informations sont transmises sur un réseau ouvert, ce qui permet à un pirate d'exploiter une faille(vulnérabilité) et de l'intercepter à travers différentes techniques. Il est fréquent de trouver difficile de repérer les attaques d'écoute. La présence d'un bug ou d'un appareil d'écoute ne peut pas avoir un impact négatif sur les performances des appareils et des réseaux, contrairement à d'autres types de cyberattaques.[W7]

II.2.2.Attaque de Modification de Données(Data Modification)

Si les acteurs malveillants ont capturé le trafic de l'entreprise, ils peuvent modifier les données contenues dans le paquet à l'insu de l'expéditeur ou du destinataire[13]. Cela signifie que certaines parties d'un message sont modifiées ou que ce message est retardé ou réorganisé afin de générer un effet non autorisé. La modification est une attaque contre l'intégrité des données originales. En somme, cela implique que des parties non autorisées non seulement accèdent aux données, mais aussi les falsifient en déclenchant des attaques de déni de service, telles que l'adaptation des paquets de données transmis ou le remplissage du réseau de fausses données.Aussi est une attaque contre l'authentification. Par exemple, un message qui stipule «

Permettez à JOHN de consulter le fichier secret X » est modifié en « Permettez à Smith de consulter le fichier secret X ».[W8]

II.2.3. IP Address Spoofing

Un acteur malveillant construit un paquet IP qui semble provenir d'une adresse valide dans l'intranet de l'entreprise. Lorsque les données circulent sur Internet, elles se déplacent en paquets. Chaque paquet contient un header (en-tête) IP. Les en-têtes IP contiennent des informations sur la source et la destination de l'adresse IP. Lorsqu'un attaquant souhaite accéder à un autre appareil, ils modifient l'adresse source d'un paquet en cours. Ainsi, le dispositif destinataire pense qu'il provient d'une source fidèle et l'accepte. Cette forme d'attaque permet aux hackers de dissimuler leurs identités et de passer outre les pare-feu. Cela peut même les aider à dissimuler leur identité de la police. [W9]

II.2.4. Attaque par Déni de Service

Une attaque DoS empêche l'utilisation normale d'un ordinateur ou d'un réseau par des utilisateurs valides. Une attaque DoS peut inonder un ordinateur ou l'ensemble du réseau de trafic jusqu'à ce qu'un arrêt se produise en raison de la surcharge. Une attaque DoS peut également bloquer le trafic, ce qui entraîne une perte d'accès aux ressources réseau pour les utilisateurs autorisés.[13]

II.2.5.Attaque de Hameçonnage

Phishing , est une pratique qui consiste à envoyer des émails frauduleux qui ressemblent à des émails provenant de sources fiables. L'objectif est de voler des données sensibles telles que les numéros de carte de crédit et les informations de connexion. C'est le type de cyberattaque le plus courant. Vous pouvez vous protéger par le biais de l'éducation ou d'une solution technologique qui filtre les e-mails malveillants.[9]

II.2.6. Logiciels malveillants(Malware)

Tout type d'altération du système informatique qui incorpore la pénétration, les chevaux de Troie, les virus et tout type de modification illicite du système informatique qui incorpore en outre la génération de codes illégaux pour modifier les codes standard à l'intérieur du système peut être qualifié d'utilisation abusive malveillante. Cela pourrait également provoquer un malheur ou des pertes incroyables liés à l'argent et devrait être évité dans tous les cas.[9]

II.3.Malware

Les logiciels malveillants sont un terme fourre-tout pour tout type de logiciel malveillant conçu pour nuire ou exploiter tout appareil, service ou réseau programmable. Les cybercriminels l'utilisent généralement pour extraire des données qu'ils peuvent tirer parti des victimes à des fins financières. [13]

II.3.1.Virus

Un virus informatique est un type de logiciel malveillant, ou malware, qui se propage entre les ordinateurs et endommage les données et les logiciels[W10]. Les virus nécessitent une action humaine pour se propager et infecter d'autres ordinateurs. Le virus se cache en s'attachant au code informatique, aux logiciels ou aux documents présents sur l'ordinateur. Une fois ouvert, le virus s'exécute et infecte l'ordinateur.[13]

II.3.2.Worms

Il installe des copies de lui-même dans la mémoire de l'ordinateur infecté. L'objectif principal d'un ver est de se répliquer automatiquement et de se propager sur le réseau d'un système à l'autre. [13]

II.3.3. Cheval de Troie(Trojan Horse)

Un cheval de Troie est un programme qui a l'air utile, mais qui contient également du code malveillant. Les acteurs malveillants utilisent des chevaux de Troie pour compromettre les hôtes. Les chevaux de Troie sont souvent fournis avec des programmes en ligne gratuits tels que des jeux informatiques, de sorte que l'utilisateur télécharge et installe le jeu avec le cheval de Troie. [13]

II.3.4.Logiciel Espion (spyware)

un programme indésirable qui surveille de manière secrète l'activité d'un utilisateur et enregistre généralement des données personnelles afin de les transmettre. [11]

II.3.5.Ransomware

Les ransomwares refusent généralement à un utilisateur l'accès à ses fichiers en chiffrant les fichiers, puis en affichant un message exigeant une rançon pour la clé de déchiffrement.Les utilisateurs sans sauvegardes à jour doivent payer la rançon pour décrypter leurs fichiers.Le paiement est généralement effectué par virement bancaire ou par crypto-monnaies telles que Bitcoin. [13]

II.3.6.Rootkit

Les rootkits (cracks) sont utilisés par les acteurs malveillants pour obtenir un accès au niveau du compte administrateur à un ordinateur.Ils sont très difficiles à détecter car ils peuvent modifier le pare-feu, la protection antivirus, les fichiers système et même les commandes du système d'exploitation pour dissimuler leur présence. Ils peuvent fournir une porte dérobée aux acteurs malveillants en leur donnant accès au PC, en leur permettant de télécharger des fichiers et d'installer de nouveaux logiciels à utiliser dans une attaque DDoS. [13]

Des outils spéciaux de suppression des rootkits doivent être utilisés pour les supprimer, ou une réinstallation complète du système d'exploitation peut être nécessaire.

II.4. Attaques réseau courantes

Lorsque des logiciels malveillants(malware) sont livrés et installés, la charge utile(payload) peut être utilisée pour provoquer diverses attaques liées au réseau. Ainsi, pour atténuer ces attaques, il est utile de comprendre les types d'attaques. En catégorisant les attaques de réseau, il est possible de traiter des types d'attaques plutôt que des attaques individuelles.

II.4.1. Attaques de reconnaissance

la collecte d'informations, Les acteurs de menaces utilisent des attaques de reconnaissance (recon) pour effectuer des découvertes non autorisées des systèmes, des services ou des vulnérabilités. Les attaques de reconnaissance précèdent les attaques d'accès ou les attaques DoS. Certaines des techniques utilisées par les acteurs malveillants pour mener des attaques de reconnaissance sont :

1.Effectuer une requête d'information sur une cible, l'acteur recherche des informations initiales sur une cible. Divers outils peuvent être utilisés, notamment la recherche Google, le site Web de l'organisation, whois, etc. [13]

2.Lancez un balayage ping du réseau cible. La requête d'informations révèle généralement l'adresse réseau de la cible. L'acteur malveillant peut désormais lancer un balayage ping pour déterminer quelles adresses IP sont actives. [13]

3.Lancez une analyse des ports(port scan) des adresses IP actives, ceci est utilisé pour déterminer quels ports ou services sont disponibles. Des exemples de scanners de ports incluent Nmap, SuperScan, Angry IP Scanner et NetScanTools. [13]

4. Exécutez des scanners de vulnérabilités(vulnerability scanners). Il s'agit d'interroger les ports identifiés pour déterminer le type et la version de l'application et du système d'exploitation qui s'exécutent sur l'hôte. Des exemples d'outils incluent Nipper, Core Impact, Nessus, SAINT et Open VAS. [13]

5. Exécutez des outils d'exploitation(exploitation tools). L'acteur menaçant tente désormais de découvrir les services vulnérables pouvant être exploités. Il existe une variété d'outils d'exploitation des vulnérabilités, notamment Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit et Netsparker. [13]

II.4.2. Attaques d'Accès (Access Attacks)

Les pirates informatiques utilisent les failles (vulnérabilités) connues sur les services d'authentification, des services FTP et des services Web pour attaquer. Ces types d'attaques visent à s'introduire dans les comptes Web, les bases de données confidentielles et d'autres

données sensibles. Des attaques d'accès sur les périphériques réseau et les ordinateurs sont utilisées par les auteurs de menaces afin de récupérer des données, d'obtenir un accès ou d'élever les privilèges d'accès au statut d'administration. Il est possible de citer diverses attaques d'accès :

- Attaques de mot de passe: Lors d'une attaque par mot de passe, l'acteur malveillant tente de découvrir les mots de passe critiques du système en utilisant diverses méthodes. Les attaques par mot de passe sont très courantes et peuvent être lancées à l'aide de une variété d'outils de piratage de mots de passe. [13]
- Attaques d'usurpation d'identité : Dans les attaques de spoofing, le dispositif de l'acteur de menace tente de se présenter comme un autre dispositif en falsifiant des données. Les attaques courantes de spoofing comprennent le spoofing d'adresse IP, de MAC et de DHCP.[13]
- Exploitation de confiance, Une attaque d'exploitation de confiance est un type de menace à la sécurité du réseau dans lequel un attaquant profite d'une relation de confiance au sein ou entre des systèmes informatiques. Dans de telles attaques, l'attaquant exploite les relations légitimes et de confiance pour éviter les contrôles de sécurité, obtenir un accès non autorisé ou mener des activités malveillantes.[W11]
- Attaque l'homme au milieu (Man-in-the-middle), est un type de cyberattaque dans laquelle l'attaquant intercepte et relaie secrètement des messages entre deux parties qui pensent communiquer directement entre elles. Les cyberattaques MitM constituent une menace sérieuse pour la sécurité en ligne, car elles donnent à l'attaquant la possibilité de capturer et de manipuler des informations personnelles sensibles, telles que les identifiants de connexion, les détails de compte ou les numéros de carte de crédit, en temps réel.[W12]

II.4.3. Attaques d'ingénierie sociale

L'ingénierie sociale est une attaque d'accès qui tente de manipuler des individus(les employés) pour qu'ils effectuent des actions ou divulguent des informations confidentielles. Certaines techniques d'ingénierie sociale sont appliquées en personne tandis que d'autres peuvent utiliser le téléphone ou Internet. Les ingénieurs sociaux s'appuient souvent sur la volonté des gens d'être utiles. Ils exploitent également les faiblesses des gens. Les attaques les plus courantes sont les suivantes :

- Pretexting : Un acteur menaçant prétend avoir besoin de données personnelles ou financières pour confirmer l'identité du destinataire. [13]

- Phishing : Un acteur malveillant envoie un e-mail frauduleux déguisé comme provenant d'une source légitime et fiable pour inciter le destinataire à installer des logiciels. malveillants sur son appareil ou à partager des informations personnelles ou financières.
- Spam : Également appelé courrier indésirable, il s'agit des e-mails non sollicités qui contiennent souvent des liens nuisibles, des logiciels malveillants ou du contenu trompeur. [13]
- Baiting : Un acteur malveillant laisse une clé USB infectée par un logiciel malveillant dans un lieu public. Une victime trouve le disque et l'insère sans méfiance dans son ordinateur portable, installant ainsi involontairement un logiciel malveillant. [13]

Les entreprises doivent éduquer leurs utilisateurs sur les risques de l'ingénierie sociale et développer des stratégies pour valider les identités par téléphone, par courrier électronique ou en personne.

II.4.4.Attaques de Déni de Services (DoS)

C'est lorsqu'un attaquant inonde intentionnellement un système, un réseau ou un site Web cible avec un grand volume de requêtes illégitimes ou de trafic malveillant. Une attaque par déni de service (DoS) crée une sorte d'interruption des services réseau pour les utilisateurs, les appareils ou les applications[13]. Nous avons plusieurs types d'attaques Dos différents, parmis eux :

- Attaques par inondations(flooding attacks),sachant que l'acteur de menace inonde le système ou le réseau cible avec une quantité massive de trafic afin de submerger ses ressources telles que la bande passante, le processeur ou la mémoire et le rendre lent ou ne répond plus. [W13]
- Attaques par Protocols, ces attaques exploitent les vulnérabilités des protocoles utilisés par le réseau, tels que tcp/ip,dns et http, pour perturber ses opérations normales. Par exemple, les attaques "Tcp Flood" inondent la cible avec un grand nombre de paquets TCP SYN, épuisant ses ressources et le rendant incapable d'établir une nouvelle connexion. [W13]
- Attaques de couche d'application, submerger l'application ou le serveur web de requêtes malveillantes. à titre d'exemple, nous prenons " HTTP Flood ", où l'attaquant inonde le site Web cible avec des requêtes HTTP excessives ou bien "DB Query attack" où l'attaquant envoie des requêtes SQL malveillantes pour perturber les opérations de la base de données. [W13]

- Attaque par déni de service distribué (DDoS) , L'efficacité des attaques DDoS réside dans l'utilisation de plusieurs systèmes informatiques compromis comme sources de trafic. Les machines exploitées peuvent être des ordinateurs et d'autres ressources situées sur le réseau, Les attaques DDoS sont exécutées avec des réseaux de machines connectées à Internet.Ces réseaux sont constitués d'ordinateurs et d'autres équipements infectés par un logiciel malveillant qui permet au pirate de les contrôler à distance. Ces dispositifs individuels sont appelés "bots" (ou zombies), et un groupe de bots s'appelle un "botnet" .Une fois qu'un botnet a été mis en place, le pirate est en mesure de diriger une attaque en envoyant des instructions à distance à chaque bot.[W13]

II.5. Politique de sécurité informatique

Une politique de sécurité des technologies de l'information (TI) implique des règles et des procédures qui permettent aux employés et aux autres parties prenantes d'utiliser et d'accéder en toute sécurité aux actifs et ressources informatiques d'une organisation. Il est important de noter qu'une politique de sécurité est bien plus qu'un ensemble de stratégies. C'est le reflet de la culture de l'entreprise, et l'adhésion de tous les membres de l'organisation est nécessaire à sa mise en œuvre réussie.

II.5.1. Politique de sécurité réseau (Network security policy)

Les correctifs critiques et autres politiques d'atténuation des menaces sont approuvés et appliqués. Les utilisateurs ne peuvent accéder aux réseaux et aux serveurs de l'entreprise que via des identifiants uniques qui nécessitent une authentification, notamment des mots de passe.Vous devez surveiller tous les systèmes et enregistrer toutes les tentatives de connexion.

Les pare-feu, les routeurs et les listes de contrôle d'accès, doivent être utilisés pour réguler le trafic réseau pour les connexions vers / depuis Internet ou d'autres réseaux .L'accès aux services de réseau internes et externes contenant des données sensibles est contrôlé par : Network access control lists (NACLs), politiques de groupes et de pare-feu, avec les plages d'adresses IP internes ne peuvent pas passer d'Internet à la DMZ ou aux réseaux internes, et Tout le trafic Internet entrant doit se terminer dans une DMZ. [14]

Les systèmes de Prevention d'intrusion sur le réseau (IPS) doivent être mis en œuvre et surveillés, les équipements réseau doivent être configurés pour fermer les sessions inactives et

l'accès aux équipements doit être limité au personnel approprié uniquement. Les autres qui ont besoin d'un accès doivent être supervisés.[14]

II.5.2.Politique de sécurité des serveurs

Les serveurs non sécurisés et vulnérables continuent d'être un point d'entrée majeur pour les acteurs malveillants. Des politiques d'installation de serveur cohérentes, la propriété et la gestion de la configuration permettent de bien faire les bases. [15]

Les serveurs doivent être enregistrés dans le système de gestion de l'entreprise. Au minimum, les informations suivantes sont nécessaires pour identifier positivement le point de contact :

- Emplacement du serveur, et le contact de secours (backup)
- Fonctions et applications principales
- Matériel et système d'exploitation/Version

L'accès aux services doit être enregistré (logged) et/ou protégé par des méthodes de contrôle d'accès telles qu'un pare-feu d'application Web, les correctifs de sécurité les plus récents doivent être installés sur le système , les services et les applications qui ne seront pas utilisés doivent être désactivés. L'accès privilégié doit être effectué sur des canaux sécurisés (par exemple, des connexions réseau cryptées utilisant SSH ou IPSec), les relations de confiance (Trust relationships) entre les systèmes constituent un risque pour la sécurité et leur utilisation doit être évitée et finalement les serveurs doivent être physiquement situés dans un environnement sécurisé et à accès contrôlé.[15]

II.5.3.Politique d'accès à distance (Remote Access Policy)

L'accès à distance à notre réseau d'entreprise est essentiel pour maintenir la productivité de notre équipe, mais dans de nombreux cas, cet accès à distance provient de réseaux qui peuvent déjà être compromis ou dont le niveau de sécurité est nettement inférieur à celui de notre réseau d'entreprise. nous devons atténuer ces risques externes au mieux de nos capacités. [16]

L'accès à distance sécurisé doit être strictement contrôlé par le chiffrement (c'est-à-dire les réseaux privés virtuels (VPN)) ,les utilisateurs autorisés protégeront leur connexion et leur mot de passe, même contre les membres de la famille et n'utiliseront pas les réseaux d'entreprise pour accéder à Internet pour les intérêts commerciaux externes, aussi tous les hôtes connectés aux réseaux internes de l'entreprise via des technologies d'accès à distance doivent utiliser le

logiciel antivirus le plus récent et on note que lorsqu'ils utilisent un ordinateur appartenant à la Société pour se connecter à distance au réseau d'entreprise de la Société, les Utilisateurs autorisés doivent s'assurer que l'hôte distant n'est connecté à aucun autre réseau en même temps, à l'exception des réseaux personnels qui sont sous leur contrôle total.[16]

II.5.4.Politique de messagerie (Email Policy)

Le courrier électronique est omniprésent dans presque tous les secteurs verticaux de l'industrie et constitue souvent la principale méthode de communication et de sensibilisation au sein d'une organisation. Dans le même temps, l'utilisation abusive du courrier électronique peut présenter de nombreux risques juridiques, de confidentialité et de sécurité, il est donc important que les utilisateurs comprennent l'utilisation appropriée des communications électroniques. [17]

Le compte de messagerie de la Société doit être utilisé principalement à des fins commerciales de la Société ; les communications personnelles sont autorisées sur une base limitée, mais les utilisations commerciales non liées à la Société sont interdites. Toutes les données de la Société contenues dans un e-mail ou une pièce jointe doivent être sécurisées conformément à la norme de protection des données aussi les e-mails sortants doivent être surveillés par la protection contre la perte de données (DLP), et les e-mails ne doivent être conservés que s'ils sont considérés comme un document d'activité (business) de l'entreprise , Tous les e-mails entrants doivent être analysés à la recherche de virus, de tentatives de phishing et de spam, il est interdit aux utilisateurs d'utiliser des systèmes de messagerie et des serveurs de stockage tiers tels que Google, Yahoo et MSN Hotmail, etc.Finalement les employés de l'entreprise ne doivent avoir aucune attente en matière de confidentialité concernant tout ce qu'ils stockent, envoient ou reçoivent sur le système de messagerie de l'entreprise.[17]

II.6.Gestion des Risques (risks management)

La gestion des cyber-risques est devenue un effort et un élément essentiel pour les entreprises. Les entreprises de tous les secteurs dépendent des technologies de l'information pour exécuter des fonctions commerciales aujourd'hui, ce qui les expose aux cybercriminels, aux erreurs des employés, aux catastrophes naturelles et à d'autres menaces de cybersécurité. Les programmes de gestion des cyber-risques peuvent aider à réduire l'impact et la probabilité des menaces.

II.6.1. Processus de Gestion des Risques de cybersécurité

Le fait de revoir régulièrement le processus permet à une entreprise d'intégrer de nouvelles informations et de réagir aux nouveaux développements dans le paysage plus large des menaces et dans ses propres systèmes informatiques.[W14]

II.6.1.1. Cadrage des risques

En définissant les risques dès le départ, les entreprises peuvent aligner leurs stratégies de gestion des risques sur leurs stratégies commerciales globales. Cet alignement permet d'éviter des erreurs inefficaces et coûteuses . Pour encadrer le risque, les entreprises définissent les éléments suivants :

- **La portée du processus :** Quels systèmes et actifs seront examinés ? Quels types de menaces seront examinés ? Sur quel calendrier le processus travaille-t-il? (par exemple, risques dans les six prochains mois, risques dans l'année prochaine, etc.) [W14]
- **Inventaire et priorisation des actifs** : quels données, appareils, logiciels et autres actifs se trouvent dans le réseau ? Lesquels de ces actifs sont les plus critiques pour l'organisation ? [W14]
- **Ressources et priorités organisationnelles:** Quels sont les systèmes de IT et les processus opérationnels les plus importants ? Quelles ressources, financières et autres, l'entreprise engagera-t-elle dans la gestion des cyberrisques ? [W14]

II.6.1.2. Évaluation des risques

Les entreprises utilisent les évaluations des risques de cybersécurité pour identifier les menaces et les vulnérabilités, estimer leurs impacts potentiels et hiérarchiser les risques les plus critiques. La plupart des évaluations suivre les éléments suivants :

- Les menaces, sont des personnes et des événements susceptibles de perturber un système informatique, de voler des données ou de compromettre la sécurité des informations. [W14]
- Les vulnérabilités, sont les failles ou les faiblesses d'un système, d'un processus ou d'un actif que les menaces peuvent exploiter pour causer des dommages. [W14]
- Les impacts, sont ce qu'une menace peut faire à une entreprise. Une cyber-menace pourrait perturber les services critiques, entraînant des temps d'arrêt et une perte de revenus. [W14]

- Le risque, mesure la probabilité qu'une menace potentielle affecte une organisation et les dommages que cette menace causerait. [W14]

II.6.1.3. Répondre aux risques

La société utilise les résultats de l'évaluation des risques pour déterminer comment elle réagira aux risques potentiels. Les réponses possibles aux risques sont les suivantes :

- **Atténuation des risques** : L'atténuation est l'utilisation de contrôles de sécurité qui rendent plus difficile l'exploitation d'une vulnérabilité ou minimisent l'impact de l'exploitation. Par exemple, placer un système de prévention des intrusions[W14]
- **Correction des risques** : La correction consiste à traiter entièrement une vulnérabilité afin qu'elle ne puisse pas être exploitée. [W14]
- **Transfert des risques :**Si l'atténuation et la correction ne sont pas pratiques, une entreprise peut transférer la responsabilité du risque à une autre partie. L'achat d'une police d'assurance cyber est le moyen le plus courant pour les entreprises de transférer les risques. [W14]

II.6.1.4. Surveillance

L'organisation surveille ses nouveaux contrôles de sécurité pour s'assurer qu'ils fonctionnent comme prévu et qu'ils satisfont aux exigences réglementaires pertinentes. En maintenant une surveillance constante, l'entreprise peut modifier son programme de cybersécurité et sa stratégie de gestion des risques en temps réel.[W14]

II.7.Dispositifs de sécurité réseau

Quelle que soit leur taille ou leur activité, toutes les entreprises sont confrontées à des problématiques d'externalisation et de sécurité informatique dans leur activité.De nombreuses menaces mettent à rude épreuve votre infrastructure et vos données, vous devez donc prendre rapidement toutes les dispositifs nécessaires pour assurer la protection.

II.7.1. Next Generation Firewall- NGFW

Les pare-feu sont un outil de sécurité standard pour la majorité des entreprises, mais dans le paysage changeant des menaces d'aujourd'hui, les pare-feu de nouvelle génération sont les seuls pare-feu capables d'offrir une protection adéquate. Un pare-feu de nouvelle génération

(NGFW) est un pare-feu d'inspection approfondie des paquets qui va au-delà de l'inspection et du blocage des ports/protocoles pour ajouter l'inspection au niveau des applications(application-level inspection), la prévention des intrusions et l'apport d'informations extérieures au pare-feu . [18]

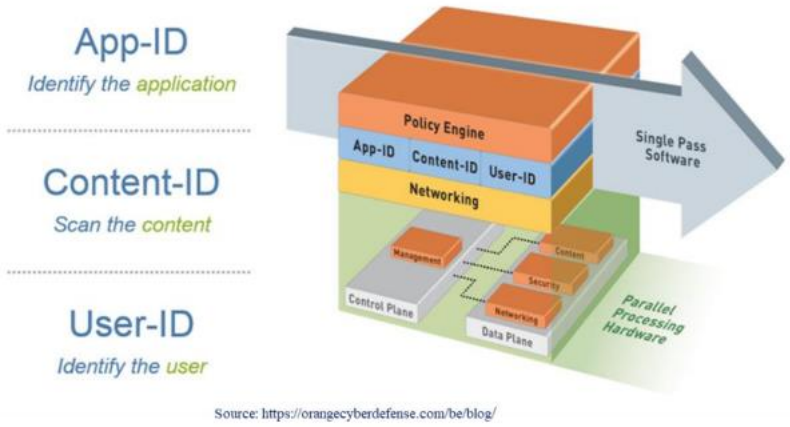

Figure II-1: Next generation firewall[21]

II.7.1.1. Caractéristiques, concepts et avantages

Les pare-feu de nouvelle génération offrent des fonctionnalités puissantes et modernes et peuvent être hébergés dans le cloud. En outre, ils intègrent des fonctionnalités supplémentaires telles que l'intelligence extérieure à leur solution, la prévention des intrusions, le contrôle des applications et l'identification par rapport aux modèles traditionnels.Pour être considéré comme un pare-feu de nouvelle génération, il doit inclure les fonctionnalités communes d'un pare-feu traditionnel, il doit disposer d'un système intégré de prévention des intrusions, et il doit permettre le contrôle des applications et valider l'identification des utilisateurs. Cependant, en raison de l'absence de réglementation de ce concept, chaque fabricant identifie les exigences minimales et ajoute des fonctionnalités qu'il juge innovantes pour se positionner et se différencier sur le marché afin de rendre sa solution à la fois plus robuste et efficace. [18]

Sa protection complète vous permet de détecter et de bloquer les attaques sophistiquées à grande échelle telles que les menaces persistantes avancées et les logiciels malveillants et elle présente une architecture axée sur les applications et les politiques des utilisateurs. La capacité d'apprentissage de l'environnement vous permet de surveiller et de gérer les événements en temps réel. Contrairement au principe des pare-feu traditionnels basés sur des règles, les pare-feu de nouvelle génération sont orientés vers l'accès à l'administration, ce qui est essentiel dans

le nouveau paradigme actuel et les défis de la mobilité, des réseaux sociaux, du cloud computing et de la collaboration. La possibilité d'inspecter l'en-tête du paquet (packet header) de données et sa charge utile (payload) améliore la détection des logiciels malveillants et atténue le trafic malveillant. Il est également possible de déchiffrer, d'analyser le trafic SSL/TLS, et de rechiffrer, agissant ainsi comme un proxy, essentiel pour les sites utilisant des connexions HTTPS sécurisées. La surveillance intelligente du trafic sur le réseau, la séparation des virus potentiels, le filtrage et la segmentation du contenu, le profilage de l'usage et la possibilité de générer des listes de menaces tous contribuent à améliorer les performances et la productivité des usagers. Ils permettent également de visualiser l'ensemble de la surface d'un attaque et offrent une intégration avec les formats cloud et multi-cloud. Grâce à sa simplicité, sa flexibilité, sa fusion des caractéristiques et son unification, vous pourrez réduire la complexité des composants de sécurité, simplifier les procédures et considérablement réduire ses coûts d'exploitation.[18]

II.7.1.2.Examples

La solution de Fortinet fournit une interface conviviale permettant une configuration rapide, granulaire et intuitive, comme le montre la Figure II-2.

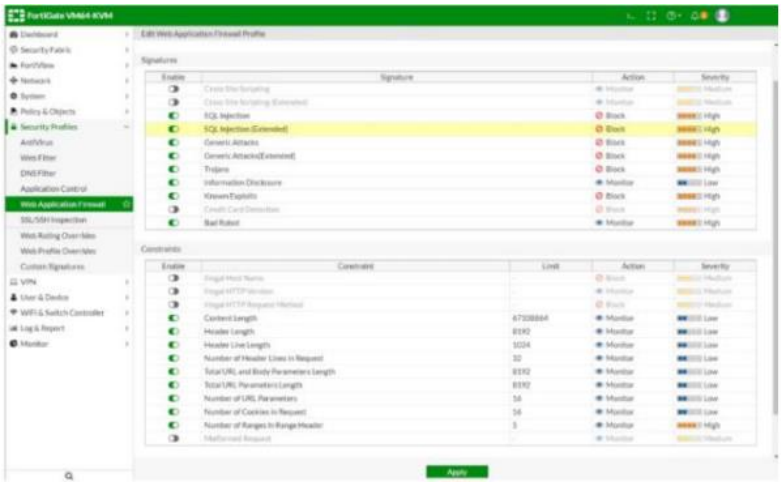

Figure II-3:Tableau de bord d'administration de FortiGate[18]

La solution Sophos offre une vision hors-bord périphérique du réseau, des applications et des utilisateurs à partir de son tableau de bord de contrôle, comme illustré dans la Figure II-4.

Figure II-5:Tableau de bord d'administration de NSCC[18]

II.7.2.Proxies

Un serveur proxy est un système ou un routeur qui fournit une passerelle entre les utilisateurs et Internet. Par conséquent, cela aide à empêcher les cyberattaquants d'accéder à un réseau privé. Il s'agit d'un serveur, appelé « intermédiaire » car il relie les utilisateurs finaux et les pages Web qu'ils visitent en ligne. [W15]

II.7.2.1.Serveurs Proxy et Sécurité du Réseau

Les proxys fournissent une couche de sécurité précieuse pour votre ordinateur. Ils peuvent être configurés comme filtres Web ou pare-feu, protégeant votre ordinateur contre les menaces Internet telles que les logiciels malveillants. Cette sécurité supplémentaire est également précieuse lorsqu'elle est associée à une passerelle Web sécurisée ou à d'autres produits de sécurité de messagerie. De cette façon, vous pouvez filtrer le trafic en fonction de son niveau de sécurité ou de la quantité de trafic que votre réseau (ou vos ordinateurs individuels) peut gérer. Certaines personnes utilisent des proxys à des fins personnelles, comme cacher leur position tout en regardant des films en ligne, par exemple. Pour une entreprise, ils peuvent cependant être utilisés pour accomplir plusieurs tâches clés telles que :

Améliorer la sécurité, sécurisez l'activité Internet des employés contre les personnes qui tentent de les espionner, équilibrez le trafic Internet pour éviter les plantages, contrôler les sites Web des employés et l'accès du personnel au bureau et économisez de la bande passante en mettant en cache les fichiers ou en compressant le trafic entrant.[W15]

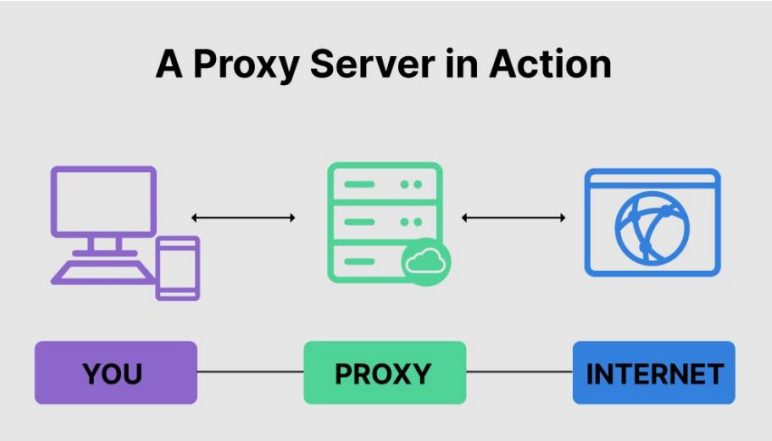

Figure II-6:Serveur proxy[W34]

II.7.3. Email Security Appliance-ESA

Le dispositif ESA est conçu pour surveiller le protocole SMTP (Simple Mail Transfer Protocol). L'ESA est constamment mis à jour par des flux en temps réel, qui détectent et corrèlent les menaces et les solutions en utilisant un système de surveillance de base de données mondiale. Ces données de renseignement sur les menaces sont extraites par l'ESA toutes les trois à cinq minutes. Voici quelques-unes des fonctions de ESA : [20]

- Bloquer les menaces connues et supprimer les e-mails contenant des liens malveillants
- Arrêter les ransomwares et zéro jour malware d'atteindre votre boîte de réception avec capture avancée Protection contre les menaces
- Techniques d'analyse avancées pour arrêter les attaques de phishing ciblées, la fraude par e-mail et la compromission des e-mails professionnels (BEC)
- Protégez les utilisateurs contre les clics sur des liens malveillants sur n'importe quel appareil et depuis n'importe quel endroit grâce à la protection des URL au moment du clic (time-of-click)
- Maintenez l'hygiène des e-mails grâce à un anti-spam et un antivirus puissants.
- Protégez vos données en appliquant des politiques granulaires de prévention des pertes de données (DLP).[19]

II.8.Technologies Défensives Intégrées dans NGFW

Se compose des fonctionnalités et des systèmes généralement intégrés dans un pare-feu de nouvelle génération .

II.8.1. Politiques de Pare-feu (Firewall policy)

Une politique de pare-feu est un ensemble de règles et de normes conçues pour contrôler le trafic du réseau entre le réseau interne d'une organisation et Internet. Il vise à prévenir l'accès non autorisé, à gérer le mouvement des données et à se prémunir contre les menaces de sécurité potentielles. Il existe des composants clés à considérer, les principaux types de politiques de pare-feu et les configurations de pare-feu à connaître et les exemples de politiques pour examiner qui offrent un contexte précieux pour créer votre propre politique de pare-feu efficace. [W16]

II.8.1.1. Composants des politiques de pare-feu

- **Authentification d'utilisateur :** Seuls les utilisateurs ou systèmes autorisés peuvent accéder au réseau via l'authentification utilisateur. [W16]
- **Règles d'accès:** Les règles d'accès, également appelées listes de contrôle d'accès (ACL), gèrent le trafic autorisé ou interdit. [W16]
- **Base de règles :** La base de règles définit les critères d'acceptation ou de rejet du trafic réseau. Cet ensemble de règles comprend des détails tels que les adresses IP source et de destination, les numéros de port et les protocoles. [W16]
- **Objets de règle :** Les objets de règle définissent des règles d'accès et intègrent des composants tels que des applications, des hôtes sources ou de destination et des réseaux. Les exemples incluent les utilisateurs, les groupes d'utilisateurs, les applications, les groupes d'applications, les pays, les points de terminaison IPv4/IPv6, les noms DNS d'hôte, etc. [W16]
- **Objets de règles basés sur les utilisateurs et les applications :** Les objets de règle Utilisateur et Groupe d'utilisateurs sont basés sur les utilisateurs et les groupes d'utilisateurs Windows Active Directory**.** [W16]
- **Objets de règle de service :** Les objets de règle de service limitent le trafic en fonction des protocoles IP, des codes ICMP ou des numéros de port TCP/UDP.[W16]

II.8.2.Politique DoS (DoS policy)

Une politique de déni de service (DoS) examine le trafic réseau arrivant à une interface de pare-feu à la recherche de modèles anormaux, ce qui indique généralement une attaque. Les politiques DoS sont vérifiées avant les politiques de sécurité, empêchant les attaques de déclencher davantage de ressources et de ralentir le dispositif de sécurité. [W17]

II.8.2.1. Anomalies de DoS

Des capteurs prédéfinis sont configurés pour des modèles de trafic anormaux spécifiques. Plusieurs anomalies prédéfinies qui peuvent être utilisées dans les politiques DoS, parmi eux[W17] :

Anomalies	Description	Seuil recommandé
tcp_syn_flood	Si le débit de paquets SYN des nouvelles connexions TCP, y compris la retransmission, vers une seule adresse IP de destination dépasse la valeur seuil configurée, l'action est exécutée.	2000 paquets par seconde.
tcp_port_scan	Si le débit de paquets SYN des nouvelles connexions TCP, y compris la retransmission, à partir d'une seule adresse IP source dépasse la valeur seuil configurée, l'action est exécutée.	1000 paquets par seconde.
udp_flood	Si le trafic UDP vers une seule adresse IP de destination dépasse la valeur seuil configurée, l'action est exécutée.	2000 paquets par seconde.
udp_scan	Si le taux d'installation des sessions UDP provenant d'une seule adresse IP source dépasse la valeur seuil configurée, l'action est exécutée.	2000 paquets par seconde.
icmp_flood	Si le nombre de paquets ICMP envoyés à une adresse IP de destination dépasse la valeur seuil configurée, l'action est exécutée.	250 paquets par seconde.
ip_src_session	Si le nombre de connexions IP simultanées à partir d'une seule adresse IP source dépasse la valeur seuil configurée, l'action est exécutée.	5000 sessions simultanées.
ip_dst_session	Si le nombre de connexions IP simultanées à partir d'une seule adresse IP source dépasse la valeur seuil configurée, l'action est exécutée.	5000 sessions simultanées.

Tableau II-1:Anomalies DoS

Pour les seuils basés sur le débit, où le seuil est mesuré en paquets par seconde, l'action "Bloquer" empêche le trafic anormal de submerger le pare-feu de deux manières :

- continu : bloque les paquets une fois qu'une anomalie est détectée et continue de bloquer les paquets tant que le débit est supérieur au seuil. Il s'agit du paramètre par défaut.
- périodique : après la détection d'une anomalie, autorisez le nombre configuré de paquets par seconde.[W17]

II.8.3.Web Application Firewall-WAF

Le pare-feu applicatif web est un pare-feu dédié destiné à filtrer et contrôler le trafic HTTP via le trafic internet entre les clients web ainsi que les serveurs applicatifs. Les pare-feu d'applications Web (WAF) sont un composant important pour une sécurité renforcée des applications. Les pare-feu réseau traditionnels fonctionnent au niveau des couches réseau et transport, ainsi que la supervision des transferts de paquets et de données. En comparaison, le WAF fournit une sécurité de couche 7 (application), généralement située entre un pare-feu de périmètre et un serveur Web ou un serveur d'applications. Contrairement à son prédécesseur, le pare-feu réseau connecté aux ports va encore plus loin en assurant la sécurité des applications servies par l'intermédiaire de l'interne. [21]

Alors que le serveur proxy protège l'identité de la machine client en utilisant l'intermédiaire, un WAF est une sorte de proxy inverse, protégeant le serveur contre l'exposition en obligeant les clients à passer par le WAF avant d'atteindre le serveur. Un WAF fonctionne selon une série de règles souvent appelées politiques. La tâche principale des WAF est de protéger des applications particulières contre les attaques Web au niveau de l'application. Dans le même temps, la technologie WAF fait de plus en plus partie de solutions de sécurité plus détaillées telles que les pare-feu de nouvelle génération (NGFW).[21]

II.8.3.1. Les Fonctions du Pare-feu Applicatif Web

Un pare-feu d'applications Web (WAF) assure la protection de vos applications Web au moyen d'un filtrage, d'une surveillance et d'un blocage de tout trafic HTTP/HTTPS malveillant circulant vers des applications Web et aide à empêcher les données non autorisées de quitter l'application, aussi appelé proxy inverse qui agit comme un intermédiaire qui protège le serveur d'applications web contre le client potentiellement malveillant.[21]

II.8.3.2. La Prévention Des Attaques à L'aide de WAF

Les pare-feu d'applications Web (WAF) sont notamment conçus pour fonctionner en combinaison avec une suite complète de produits de sécurité tels que les pare-feu traditionnels ainsi que les systèmes de prévention des intrusions (IPS). En même temps, ils sont très efficaces pour bloquer certains types d'attaques, les cyberattaques les plus répandues dans les applications que les WAF aident à prévenir sont [21]:

Attaques	Description
SQL Injection	est une sorte d'attaque qui insère une requête SQL qui permet au pirate de lire des données confidentielles, d'usurper l'identité, de modifier les données et parfois d'émettre des ordres au système d'exploitation.
Cross-Side-Scripting XSS	est une sorte d'injection, où des scripts malveillants sont injectés dans les sites Web de confiance. Les pirates envoient du code malveillant, souvent un script côté navigateur, à l'utilisateur final, s'il est exposé, l'utilisateur n'aura aucune méthode pour comprendre que le script ne doit pas être fiable et l'exécute. Un script malveillant peut accéder à des informations sensibles ou en modifier le contenu
Web Scraping	Le Web Scraping est une technique permettant d'obtenir certaines informations du site Web, en les utilisant fréquemment pour leurs propres sites Web. Un WAF peut empêcher les scripts ou les machines d'obtenir des données à partir d'un site Web

Tableau II-2:Prévention des attaques à l'aide d'un WAF

II.8.4. Systèmes de prévention des intrusions-IPS

Les IPS sont des solutions de sécurité avancées qui détectent et empêchent de manière proactive les activités non autorisées ou malveillantes qui compromettraient l'intégrité de votre réseau**.** [W18]

II.8.4.1.Le Fonctionnement de IPS

Les systèmes de prévention des intrusions se composent de plusieurs composants clés. Tout d'abord, il y a des capteurs placés stratégiquement sur votre réseau pour surveiller le trafic. Ces capteurs collectent des données et les envoient au moteur de détection, où des algorithmes sophistiqués analysent les modèles et les comportements. Si une menace est identifiée, le mécanisme de prévention prend des actions (bloque-log) pour arrêter la menace dans son élan.[W18]

II.8.4.2. Comparaison des Méthodes de Détection

- **Signature-based detection :** IPS compare le trafic entrant à une base de données de modèles d'attaque connus. S'il trouve une correspondance, il prend des mesures immédiates pour bloquer ou atténuer la menace. [W18]
- **Anomaly-based detection :** est une autre technique cruciale. Considérez-le comme un profileur comportemental. IPS surveille le comportement normal du réseau et établit

une base de référence. Lorsque l'activité s'écarte considérablement de cette ligne de base, elle lève un drapeau. Par exemple, si un utilisateur commence soudainement à évaluer des fichiers sensibles qui n'ont jamais été évalués auparavant, l'IPS prend des actions.[W18]

II.8.5. Réseaux Privés Virtuels-VPNs

Pour sécuriser le trafic réseau entre les sites et les utilisateurs, les organisations utilisent des réseaux privés virtuels (VPN) pour créer des connexions réseau privées de bout en bout. Un VPN est virtuel en ce sens qu'il transporte des informations au sein d'un réseau privé, mais ces informations sont en fait transportées sur un réseau public. Un VPN est privé dans la mesure où le trafic est crypté pour garder les données confidentielles lorsqu'elles sont transportées sur le réseau public.[22]

II.8.5.1.Remot Access VPN

Les VPN sont devenus la solution logique pour la connectivité à distance pour de nombreuses raisons. Comme le montre la figure, les VPN d'accès à distance permettent aux utilisateurs distants et mobiles de se connecter en toute sécurité à l'entreprise en créant un tunnel chiffré. Les utilisateurs distants peuvent répliquer en toute sécurité leur accès de sécurité d'entreprise, y compris les applications de messagerie et de réseau. Les VPN d'accès à distance permettent également aux sous-traitants et aux partenaires d'avoir un accès limité aux serveurs, pages Web ou fichiers spécifiques selon les besoins. Cela signifie que ces utilisateurs peuvent contribuer à la productivité de l'entreprise sans compromettre la sécurité du réseau. Les VPN d'accès à distance sont généralement activés dynamiquement par l'utilisateur lorsque cela est nécessaire. Les VPN d'accès à distance peuvent être créés à l'aide d'IPsec ou de SSL. Comme le montre la figure, un utilisateur distant doit initier une connexion VPN d'accès à distance.[22]

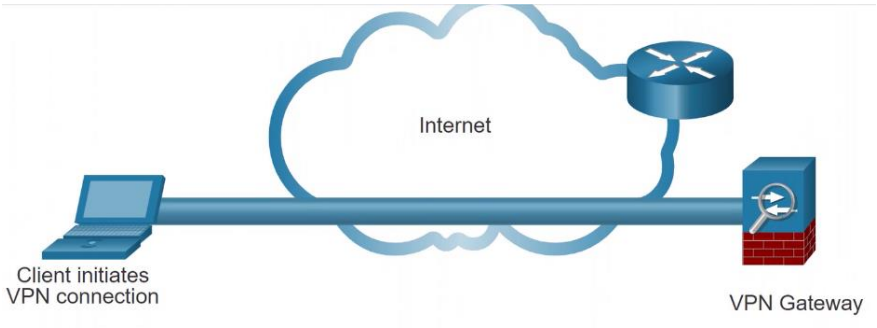

Figure II-7: VPN d'accès à distance[22]

II.8.5.2. Site-to-Site VPN

Les VPN site à site sont utilisés pour connecter des réseaux sur un autre réseau non fiable tel qu'Internet. Dans un VPN site à site, les hôtes finaux envoient et reçoivent du trafic TCP/IP normal non chiffré via un périphérique de terminaison VPN. La terminaison VPN est généralement appelée passerelle VPN. Un périphérique de passerelle VPN peut être un routeur ou un pare-feu, comme illustré sur la figure. Le trafic est uniquement chiffré entre les passerelles. Les hôtes internes ne savent pas qu'un VPN est utilisé.[22]

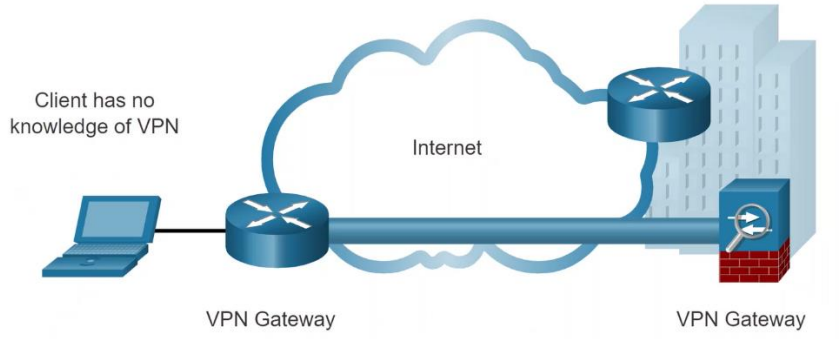

Figure II-8: VPN site à site[22]

II.9. Conclusion

Dans ce chapitre, nous avons abordé plusieurs aspects importants de les solution de la sécurité informatique. Nous avons commencé par présenter les Attaques réseau courantes et leurs différents types, la gestion des risques et menaces informatique. De plus, nous avons examiné en détail les solutions les plus répandues dans le milieu des entreprises, en mettant en évidence leurs fonctionnalités et leurs avantages respectifs.

Chapitre III : Mise en Place et Simulation

III.1.Introduction

Dans ce chapitre, nous présenterons les étapes de l'implémentation de notre solution proposée ci-dessous.Nous commencerons par décrire l'environnement de développement et l'architecture utilisée, puis nous expliquerons les différentes étapes suivies pour la configuration de cette architecture , le réalisation de DMZ , AD Replication et nous finirons par la mise en place d'un VPN-SSL.

III.2.Problématique

Auparavant,l'architecture réseau de la DG-Nesda ne posséde pas d'une zone démilitarisée (DMZ) ce qui est considéré comme un grand risque en terme de sécurité informatique et entraine la possibilité de recevoir des cyber-attaques.

Ainsi , NESDA est une organisation géographiquement dispersée,61 agence à travers 48 wilayas doivent consulter le seul Domain Controller(AD DS) situé au DG-Alger pour bénificier de ces services,de sorte que toutes les requêtes doivent être acheminées vers le DC central ce qui peut entraîner une **congestion du réseau**, aussi les utilisateurs situés loin du DC central peut rencontrer **une latence** accrue lors de l'accès aux ressources ou aux services ,et le plus important c'est le fait d'avoir un serveur DC sur un seul site (dans une grande organisation) peut poser un risque de sécurité, si le serveur est **compromis** (DCs contiennent des données trés sensibles) toutes les données et tous les services sont à risque.

Le besoin des employés de la DG-Nesda de consulter parfois avec **une maniére sécurisée** des ressources internes (internal network) qui peuvent ne pas etre sur une connexion internet publique, lorqu' ils sont en dehors du siege de l'entreprise.

- **Solutions proposées**

✓ Création d'une zone démilitarisée DMZ avec implementation des régles de sécurité correspondantes en utilisant le pare-feu FortiGate ;

✓ Amélioration de la protection contre les attaques online sur le pare-feu FortiGate;

✓Optimisation de trafic WAN entre les branches de l'entreprise et protéger le serveur DC contre les compromissions en déployant le processus "Active Directory Replication" au sein des agences des wiliayas;

✓Fournir un accés à distance "sécurisé" et peu coûteuse au ressources internes par la mise en place d'un VPN-SSL

✓Amélioration des performances et la vitesse de réseau Nesda ,simplifier l'administration en créant un réseau pour les ressources internes

III.3.Présentation de l'environnement de travail

Pour l'implémentation de notre projet, nous avons utilisé le logiciel Vmware workstation pro comme environnement de développement et d'implementation .

III.3.1. Environnement matériel

III.3.1.1.HP Elite Book 840 G3

- **Système d'exploitation :** Windows 10 Professionnel.
- **Processeur :** Intel(R) Core (TM) i7 6500U CPU @ 2.50GHZ
- **RAM :** 16GB
- **Disque Dur :** SSD 256 GO

III.3.2. Environnement logiciel

III.3.2.1.VMware workstation pro 2023

VMware Workstation Pro 2023 est une application qui fonctionne comme middleware, une combinaison de logiciel et de médiateur matériel et un outil de gestion des ressources. Il s'agit de l'approche idéale pour comprendre les connexions et enquêter et évaluer divers types d'applications liées au réseau avant le déploiement et l'utilisation dans les circonstances réelles, et nous permet de configurer un certain nombre de systèmes d'exploitation distincts à l'intérieur d'un système d'exploitation utilisé et de créer une liaison réseau informatique entre eux.[W19]

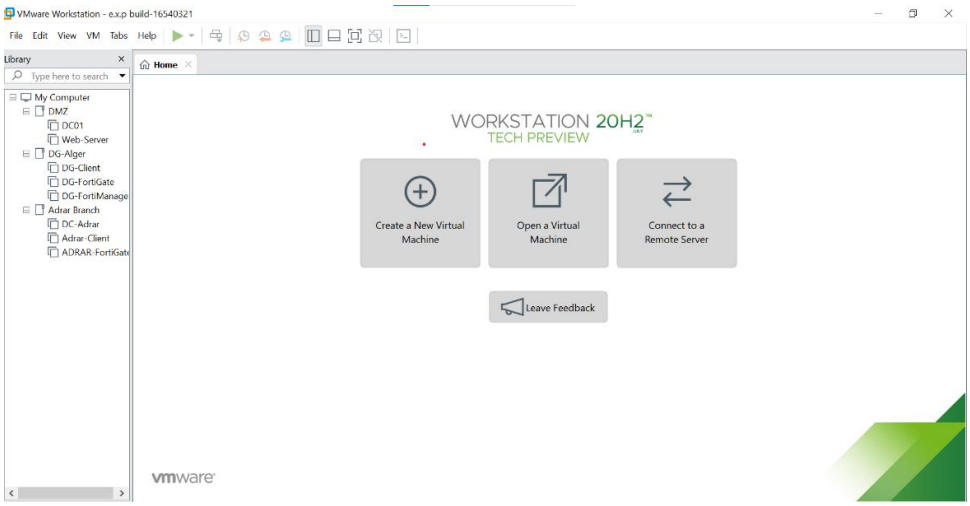

Figure III-1: L'interface graphique Vmware

III.3.2.2.Presentation de FortiGate Next Generation Firewall

Les pare-feu FortiGate sont une gamme de solutions de sécurité réseau proposées par Fortinet, l'un des principaux fournisseurs de solutions de sécurité réseau.Ils protègent les réseaux contre

un large éventail de cyber-menaces, telles que les logiciels malveillants, les virus et les attaques de pirates. Ils utilisent des renseignements avancés sur les menaces et l'apprentissage automatique pour détecter et bloquer les menaces connues et inconnues en temps réel. Offrent également une sécurité multicouche en intégrant la sécurité du réseau, du Web et des e-mails dans une solution unique. Cela permet aux entreprises de protéger leurs réseaux contre de nombreuses menaces, notamment les logiciels malveillants, le spam et les phishing attacks. [W20]

III.3.2.3.Presentation de Apache Web Server

Apache HTTP Server, est un logiciel de serveur Web gratuit et open-source conçu pour fournir du contenu Web via Internet et le serveur Web le plus populaire sur Internet[W22]

Il sert d'intermédiaire entre le serveur et les machines clientes, en gérant les requêtes des navigateurs et en fournissant le contenu du serveur sur le Web[W21]

III.3.2.4.Presentation de Samba File Server

Samba est un logiciel open source,développé pour un partage de fichiers et d'impression rapide et sécurisé pour tous les clients utilisant le protocole SMB[W24]. était à l'origine utilisé pour les fichiers, l'impression et d'autres services pour les systèmes d'exploitation Microsoft Windows. Les serveurs Samba prennent en charge les systèmes d'intégration Windows, Linux et Unix, ce qui permet de partager des fichiers ou d'utiliser des imprimantes sur n'importe quel système d'exploitation. Depuis le lancement de la version 4, les serveurs Samba Unix et Linux ont pris le rôle de contrôleurs de domaine Active Directory, qui permettent une autorisation et une authentification centralisées pour les ordinateurs et les utilisateurs. Les serveurs Samba sont composés de plusieurs modules, permettant de configurer des protocoles SMB ou CIFS.[W25]

III.3.2.5.Presentation de Windows Server 2019

Windows Server fait partie intégrante des environnements informatiques modernes, fournissant l'épine dorsale de nombreux services et applications d'entreprise. Il est conçu pour fonctionner de manière transparente avec d'autres produits et services Microsoft. Windows Server inclut des fonctionnalités telles qu'Active Directory, le serveur DNS, le serveur DHCP et les services de fichiers et de stockage.[W23]

III.3.2.6.Les Machines Virtuelles Utilisées

Noms	**Sys d'exploitation**	**RAM**	**CPU**
DCO1	Winds server 2019	3 GB	2 Core
DC-Adrar	Winds server 2019	3 GB	2 Core
Web/File Server	Linux-Ubuntu	4 GB	2 Core

DG-FortiGate	FortiOS 6.4.15/7.2.0	2 GB	1 Core
Adrar-FortiGate	FortiOS 6.4.15/7.2.0	2 GB	1 Core
DG-Client	Windows 10	3 GB	2 Core
Adrar-Client	Windows 10	3 GB	2 Core
Remote User	Windows 10	3 GB	2 Core
Attack-Test	Linux-Kali	3 GB	2 Core

Tableau III-1:Caractéristiques Des Machines Virtuelles Utilisée

III.4.Architecture Réseau Réalisée

III.4.1.Le Schéma de l'architecture

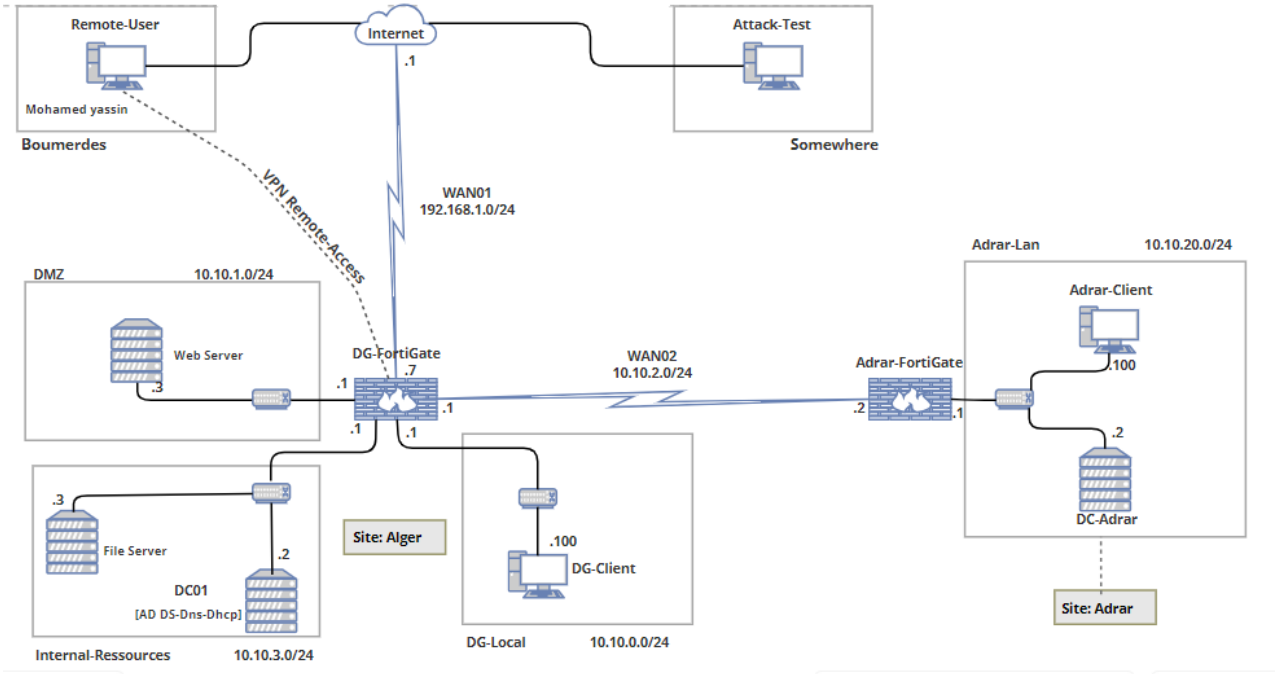

Figure III-2:Architecture Réalisée

III.4.2.Le plan d'adressage

Machines-Virt	Interfaces	Adresse ip	Réseau
DCO1	Ethernet	10.10.3.2	Internal ressources
File Server	Ethernet	10.10.3.3	Internal ressources
Web Server	Ethernet	10.10.1.3	DMZ
DC -Adrar	Ethernet	10.10.20.2	Adrar-Lan
Adrar-Client	Ethernet	10.10.20.100	Adrar-Lan
Adrar-FortiGate	Port 1	10.10.2.2	WAN2

	Port 2	10.10.20.1	Adrar-Lan
DG-Client	Ethernet	10.10.0.100	DG-Local
DG-FortiGate	Port 1	192.168.1.7	WAN1
	Port 2	10.10.0.1	DG-Local
	Port 3	10.10.1.1	DMZ
	Port 4	10.10.2.1	WAN2
	Port5	10.10.3.1	Internal ressources

Tableau III-2: Le Plan d'adressage

III.4.3.Configuration des Interfaces sur les pare-feu FortiGate

Nous avons attribué les adresses ip au ports , et permis l'accés de certains protocoles selon le besoin.

- **Sous La Machine DG-FortiGate**

```
DG-FortiGate # config sys int
DG-FortiGate (interface) # edit  port1
DG-FortiGate (port1) # set mode static
DG-FortiGate (port1) # set ip 192.168.1.7/24
DG-FortiGate (port1) # set role  wan
DG-FortiGate (port1) # next
DG-FortiGate (interface) # edit  port2
DG-FortiGate (port2) # set ip 10.10.0.1/24
DG-FortiGate (port2) # set allowaccess https http  ping
DG-FortiGate (port2) # set role  lan
DG-FortiGate (port2) #
```

Figure III-3: Configuration des ports 1 et 2 sous DG-FortiGate

```
DG-FortiGate (port2) # next
DG-FortiGate (interface) # edit  port3
DG-FortiGate (port3) # set ip 10.10.1.1/24
DG-FortiGate (port3) # set role  dmz
DG-FortiGate (port3) # set allowaccess ping
DG-FortiGate (port3) # next
DG-FortiGate (interface) # edit  port4
DG-FortiGate (port4) # set ip 10.10.2.1/24
DG-FortiGate (port4) # set allowaccess ping
DG-FortiGate (port4) # set role  wan
DG-FortiGate (port4) # _
```

Figure III-4: Configuration des ports 3 et 4 sous DG-FortiGate

```
DG-FortiGate (interface) # edit  port5
DG-FortiGate (port5) # set ip 10.10.3.1/24
DG-FortiGate (port5) # set role  lan
DG-FortiGate (port5) # set allowaccess ping
DG-FortiGate (port5) # end
```

Figure III-5: Configuration de ports 5 sous DG-FortiGate

- **Sous La Machine Adrar –FortiGate**

```
Adrar-FortiGate # config sys int
Adrar-FortiGate (interface) # edit  port1
Adrar-FortiGate (port1) # set mode static
Adrar-FortiGate (port1) # set ip 10.10.2.2/24
Adrar-FortiGate (port1) # set allowaccess ping
Adrar-FortiGate (port1) # set role  wan
Adrar-FortiGate (port1) # next
Adrar-FortiGate (interface) # edit  port2
Adrar-FortiGate (port2) # set ip 10.10.20.1/24
Adrar-FortiGate (port2) # set allowaccess https http  ping
Adrar-FortiGate (port2) # set role  lan
Adrar-FortiGate (port2) # _
```

Figure III-6: Configuration des ports 1 et 2 sous Adrar-FortiGate

III.5.Installation et Configuration de Réseau "Internal Ressources"

Nous avons crée le réseau "internal ressources" seulement pour les ressources internes de l'entreprise , à pour objectif d'améliorer les performances et la vitesse du réseau, simplifier l'administration et de faciliter la gestion de notre réseau et également pour améliorer la sécurité, de sorte que même si une partie du réseau est compromise, l'impact ne peut être contenu que dans cette partier.

Maintenent après le déploiement de ce réseau , nous avons besoin reconfiguré le grand réseau pour les Services AD DS ,Dns et Dhcp et fournir l'accés pour le serveur de fichiers.

III.5.1. Autorisation des Trafics

Par défaut, FortiGate Firewall " bloque " tous le trafics quelque soit les services .

Nous avons accédé au GUI de "DG-FortiGate" via le navigateur web sur la machine "DG-Client" par l'adresse ip 10.10.0.1 et permettre le passage de trafics depuis le réseau "DG-Local" vers Le réseau "Internal Ressources" seulement pour les besoins de l'entreprise ,par l'ajoute des "politiques de sécurité" sur le par-feu DG-FortiGate .

- Autorise les Clients de "DG-local" de bénificier des Sevices de AD DS,Dhcp et Dns contenant sur DC01

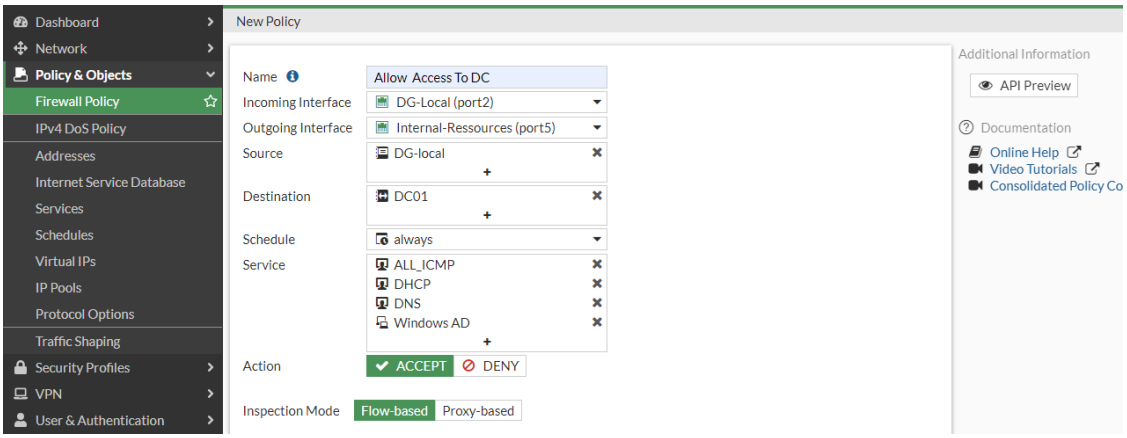

Figure III-7: ajoute une politique de sécurité pour windows sever 2019

- Autorise les Clients de "DG-local" Consulter les fichiers Nesda par l'accés au serveur de fichier , Le Serveur de fichier Samba écoute sur le port 445 (Smb protocol) pour ce la nous avons autorisé just les services SMB (icmp pour le ping).

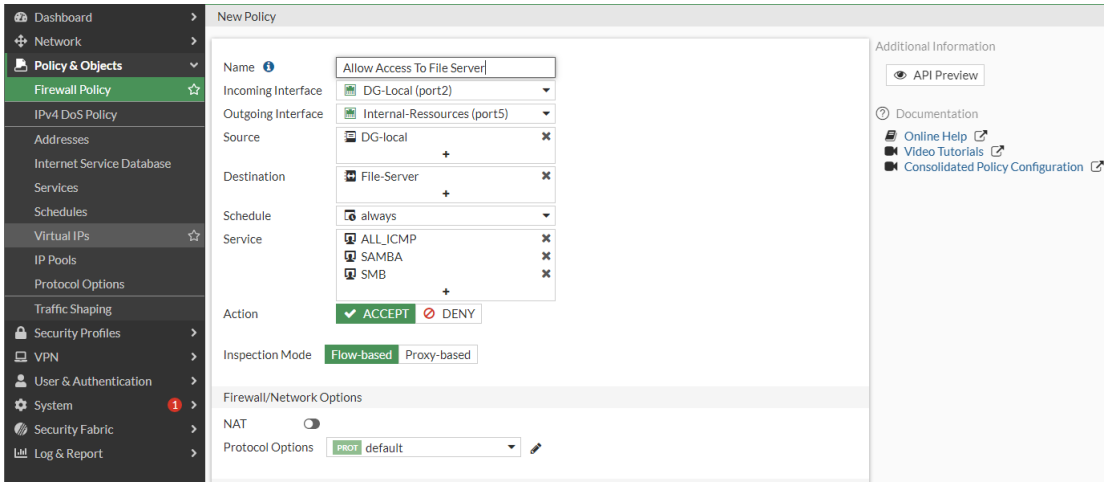

Figure III-8 : ajoute une politique de sécurité pour le serveur de fichier samba

III.5.2. Installalation et Configuration de Ad DS,DNS et Dhcp sous Windows Server

Nous avons mis en place un Serveur dhcp pour la distribution dynamique des adresses ip , le serveur dns pour la résolution de nom et AD DS pour la gestion du domain de l'entreprise .

- On doit commencer par AD DS ,sur DC01 nous avons créé un nouveau domaine sous le nom " nesda.lan " passont par :

Server manager → promote this server to a domain controller → add new forrest

Figure III-9: Spécifier les information de domaine

- On doit ajouter nouveau utilisateur dans le domaine "nesda.lan" suivant le chemin : Tools→AD user and computers → new user

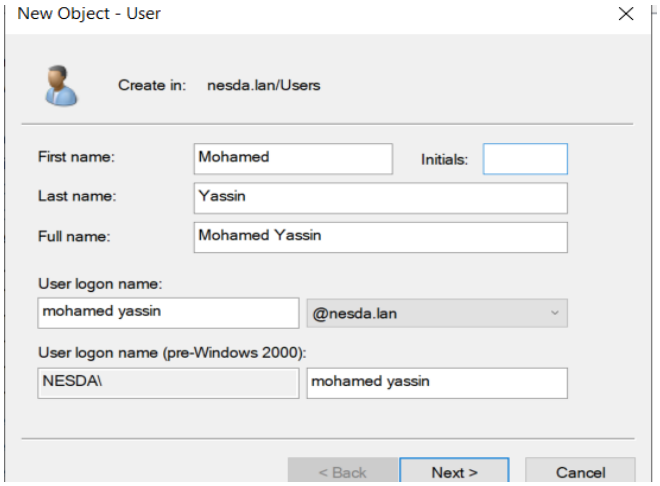

Figure III-10: Spécifier les information d'utilisateur

- Sur la machine DG-Client (réseau DG-Local), nous avons rejoint cette machine au domaine "nesda.lan" : Settings→Système→about→advanced système settings

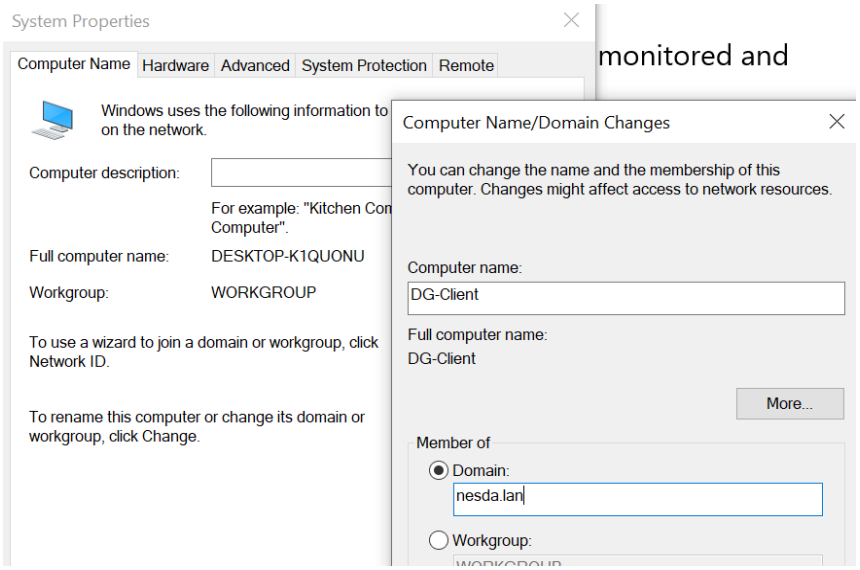

Figure III-11: changer le domaine et le nom de DG-Client

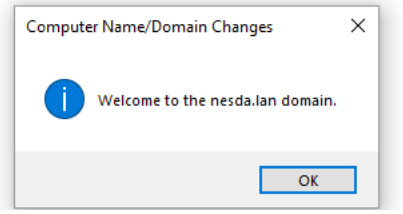

Figure III-12: validation de rejoint

- La machine DG-Client est ajouté automatiquement au niveau de AD DS ce qui valide le succés de l'opération.

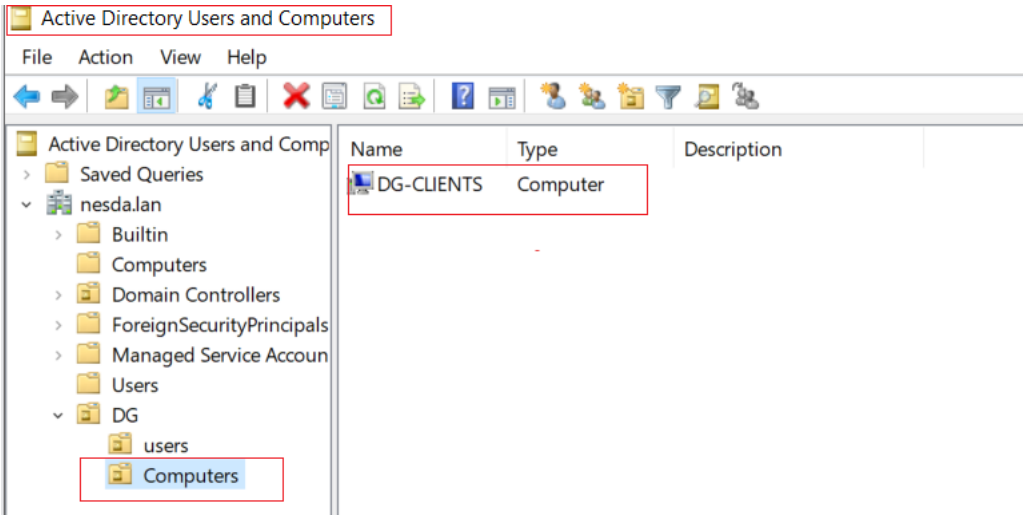

Figure III-13: Présentation de DG-Client au sein de AD DS

- Puis,nous avons passé sur la configuration de Dhcp par la création de nouveau pool d'adresse ip pour le réseau DG-local et spécifier les limites de ce pool (start-end) : Server manager → tools → dhcp → new scoop

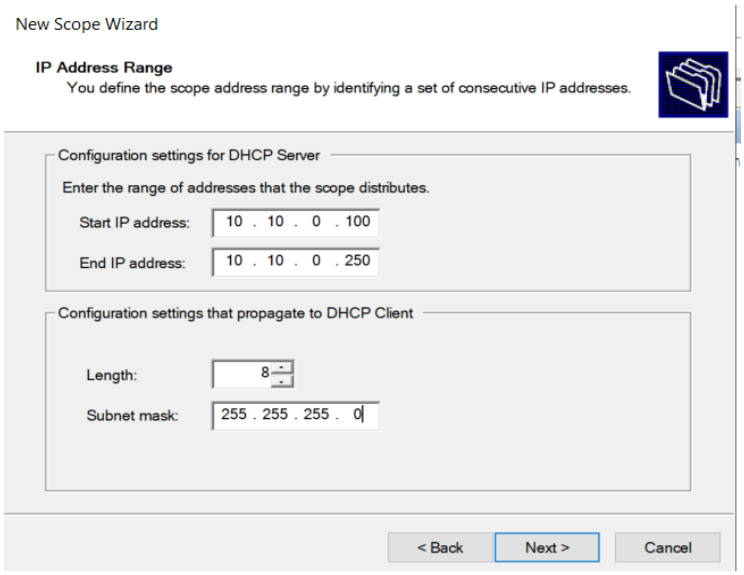

Figure III-14: configuration de pool d'adresse ip

- Après, nous avons ajouté un serveur Dns et créer un record de type "host" pour le serveur Web :Server manager → tools → Dns

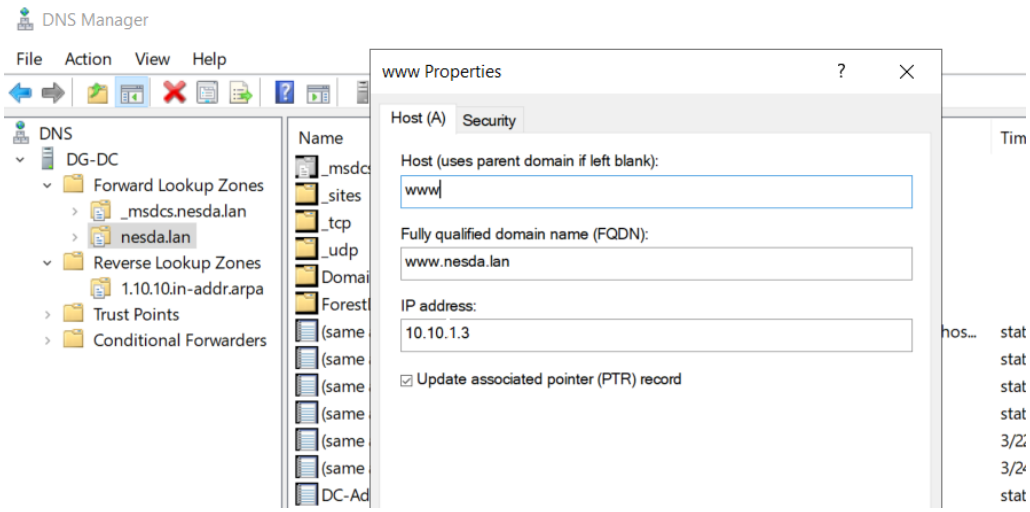

Figure III-15: Configuration de dns

- Teste de résolution de nom depuis le client "DG-Client" par la commande " nslookup" Ce qui valide le bon fonctionnement des Service Dns,Dhcp et AD DS.

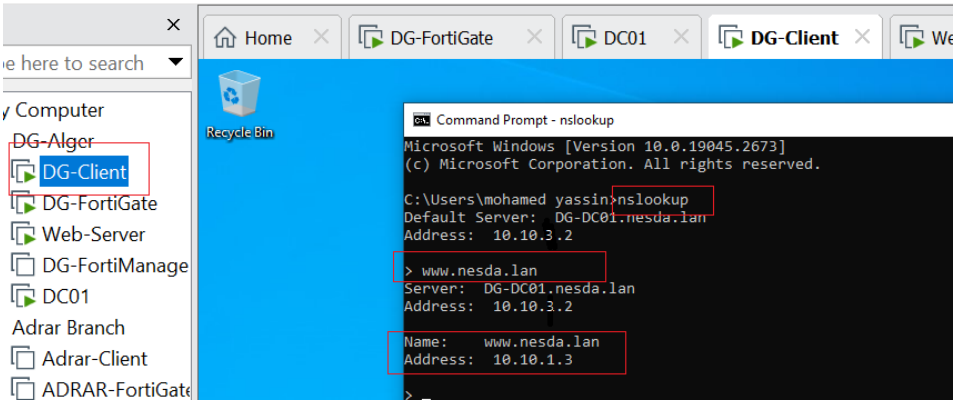

Figure III-16: teste la résolution des noms

- Puis, nous avons testé la possibilité que les employés de l'entrprise avoir un accés au serveur de fichier situé au réseau "Internal Ressources" , sur la machine DG-Client : File explore→bare de recharche(double back-slash+ @ ip de serveur)→ \\10.10.3.3

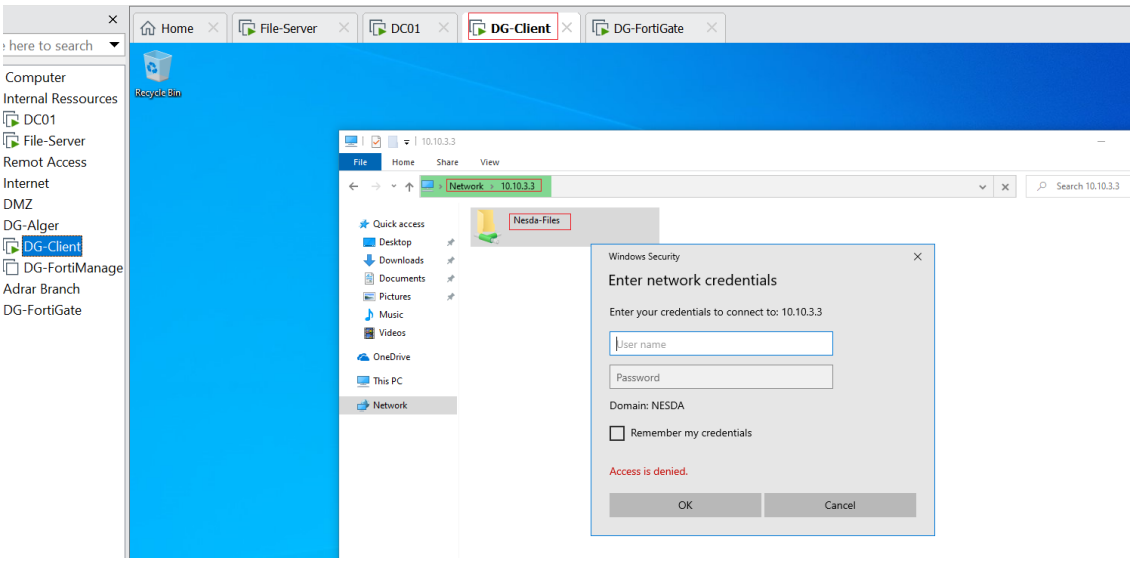

Figure III-17: Tentative d'accés au serveur de fichiers

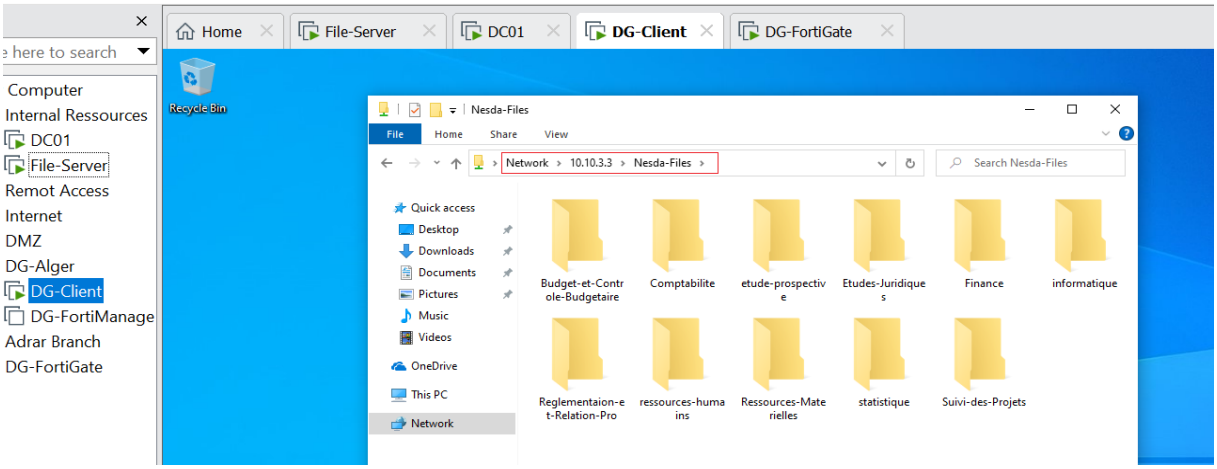

Figure III-18:Accés réusssir à tous les dossier de Nesda

III.6.Implémentation de AD Replication pour l'Agence de la Wilaya Adrar

Après avoir mis en place un Serveur Windows 2019 sur le Site "Adrar" et installer dedans AD DS , nous avons commencé l'implémentation et la configuration de AD replication .

III.6.1. Routage et Autorisation des Trafics

Nous avons crée des politique de sécurité sur "DG-FortiGate" et "Adrar-FortiGate" pour seulement le passage des Donneés nécessaire entre les deux réseaux "Internal-ressources" et " Adrar-Lan ".

III.6.1.1.Sous la Machine Adrar-FortiGate

- Autoriser le passage de paquets sortants de "DC-Adrar" (Adrar-Lan) vers "DC01" (Internal-ressources) sauf pour les services Active-Directory

Figure III-19: autorisation de trafics sortans de DC-Adrar vers DC01

Puis, nous devons autoriser le trafics entrants au réseau Adrar-lan et que pour DC-Adrar provenait de DC01 (Internal-ressources)

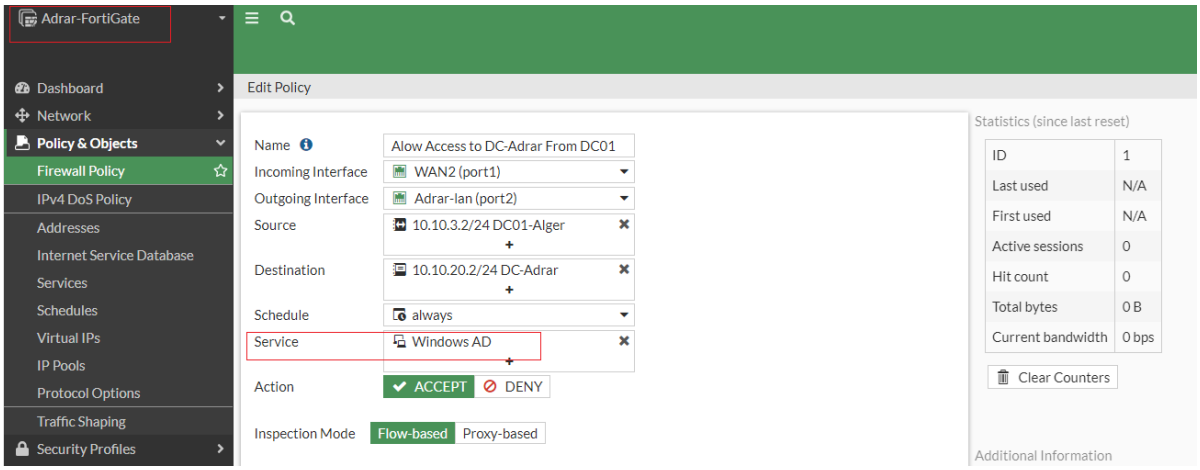

Figure III-20: autorisation de traffics entrants à Adrar-lan provenant de Internal-ressources

- On doit ajouter une route par défaut parce que " Internal-ressources" est un réseau distant

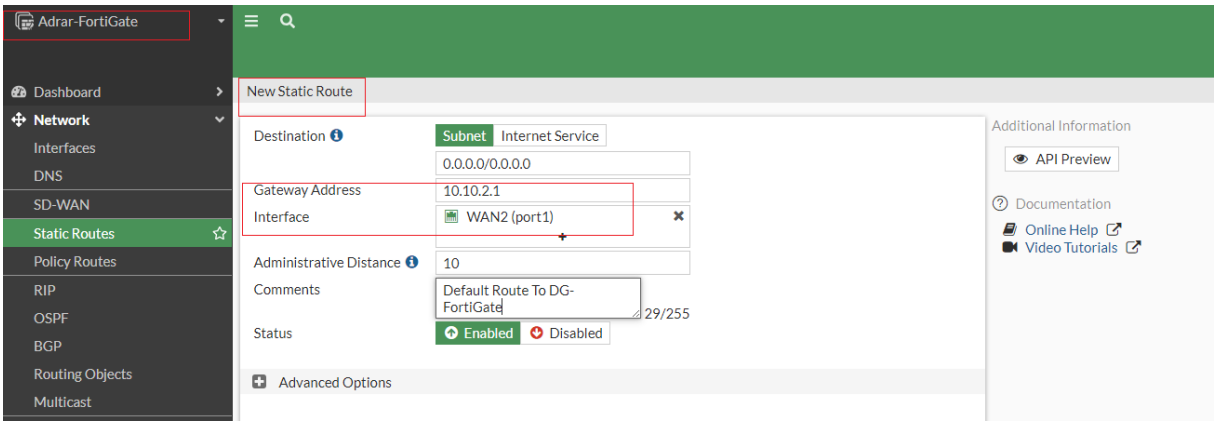

Figure III-21: Création d'une route par défaut sur Adrar-FortiGate

III.6.1.2.Sous la Machine DG-FortiGate

- Au premier lieu, nous avons ajouté une route static vers le réseau "Adrar-lan"

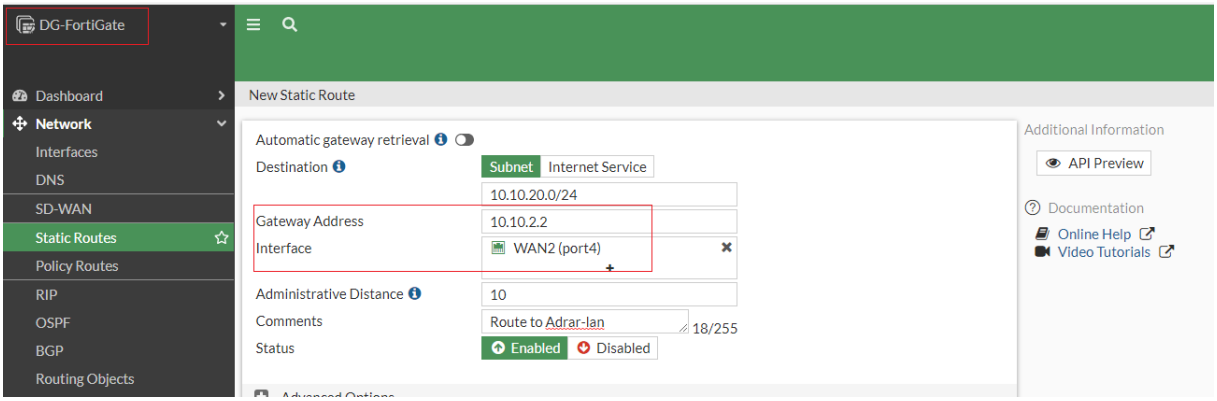

Figure III-22: création d'une route statique vers Adrar-lan

- Puis, on a pérmet l'accés au DC01 depuis le réseau "Adrar-lan" et uniquement pour les services nécessaires Active Directory

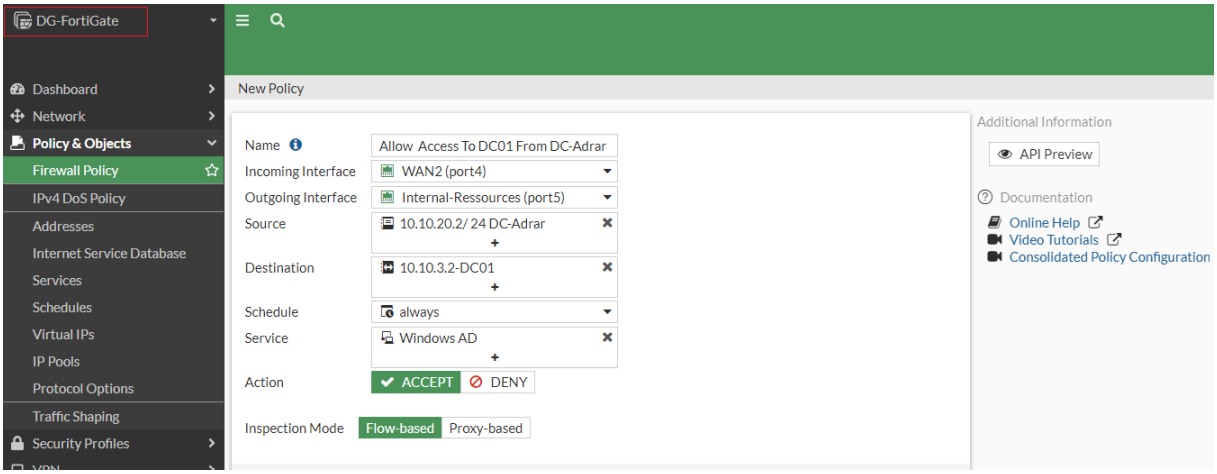

Figure III-23: Autorisation d'accés au DC01 depuis DC-Adrar

- Au dernier lieu, nous avons Pérmet l'envoie des mises à jour (updates) de DC01 vers DC-Adrar

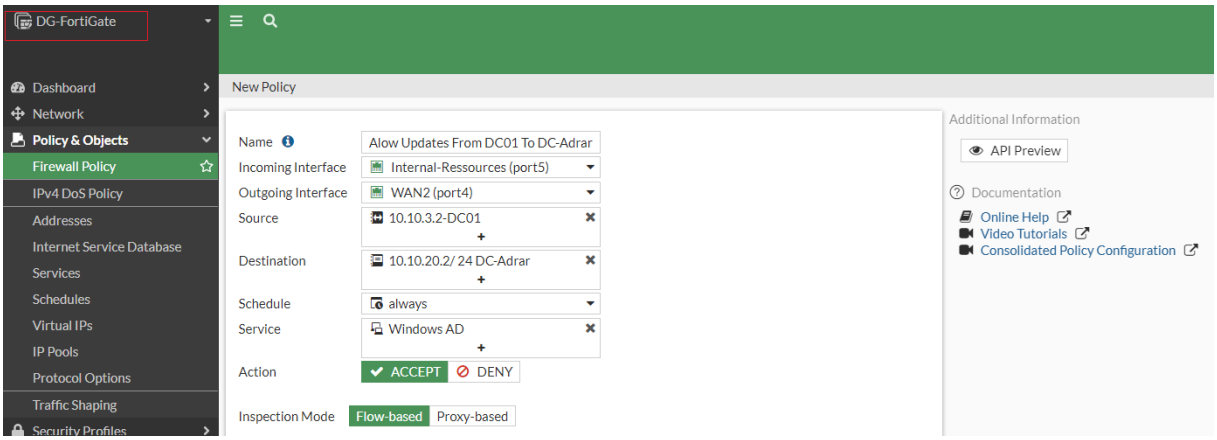

Figure III-24: Autorisation des mises à jour vers DC-Adrar

III.6.1.3.Teste de connectivité

- De DC01(réseau DMZ) → DC-Adrar (réseau Adrar-lan)

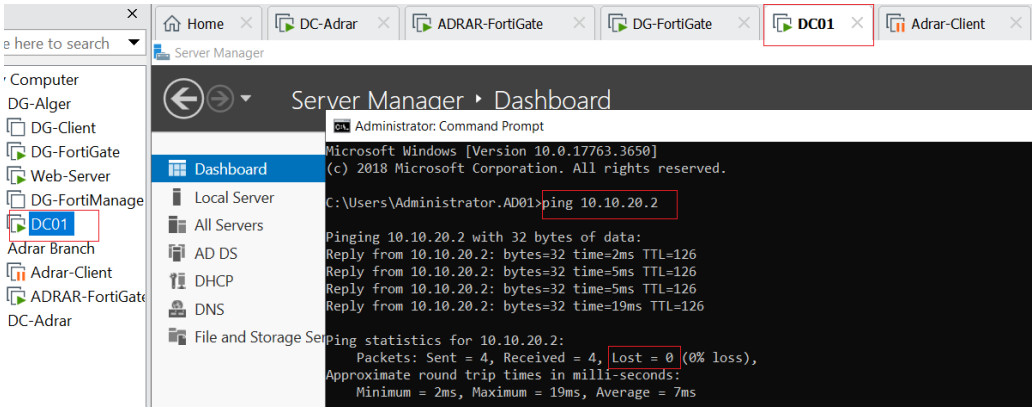

Figure III-25: teste depuis DC01 vers DC-Adrar

- De DC-Adrar (réseau Adrar-lan) vers DC01(réseau DMZ)

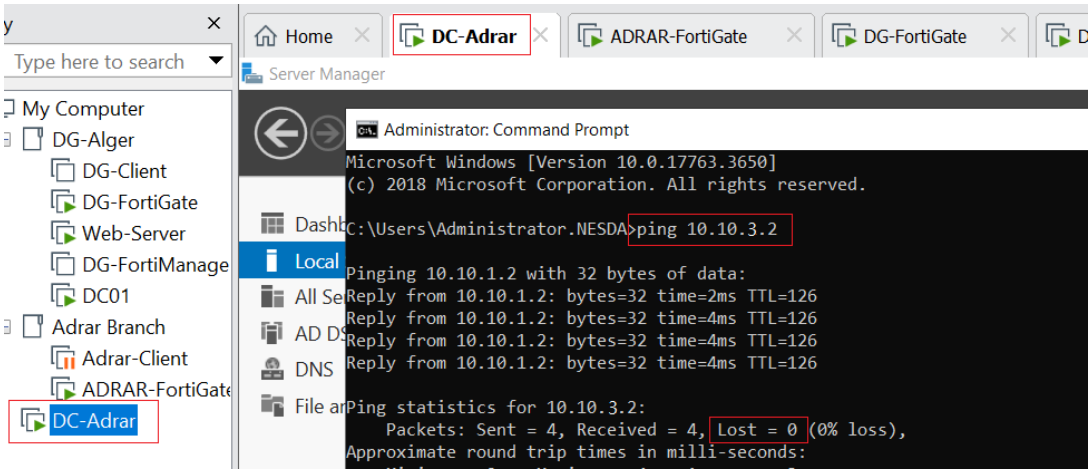

Figure III-26: Teste depuis DC-Adrar vers DC01

III.6.2.Rejoindre " DC-Adrar " au Domaine "nesda.lan"

Nous avons rejoint le "Domain controller" du site Adrar nommé par Adrar-DC au domaine parent de nesda "nesda.lan" .

Sous la machine DC-Adrar : Server manager→promote this server to a domain controller→add a domain controller to an existing domain .

On doit taper "nesda.lan" puis entrer les credentials

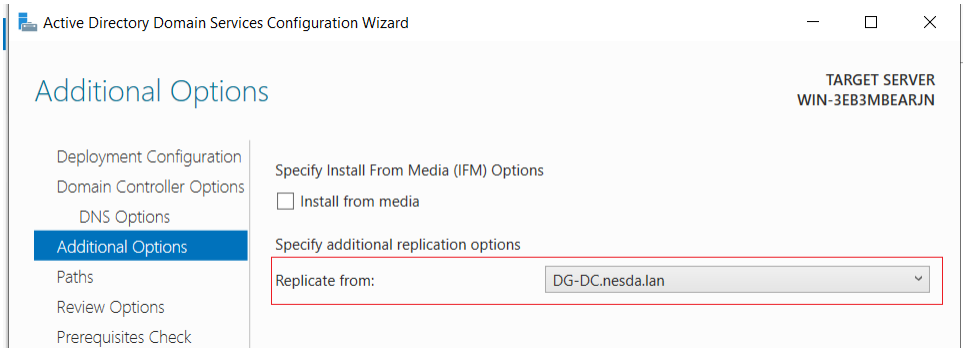

Figure III-27: L'ajout de DC-Adrar au domaine parent nesda.lan

III.6.3.La Création et Configuration de AD Sites et AD Subnets

- Nous avons crée le site "Adrar" au niveau de DC01 (Alger) :

  Tools → AD Sites and Services → Sites → New Site

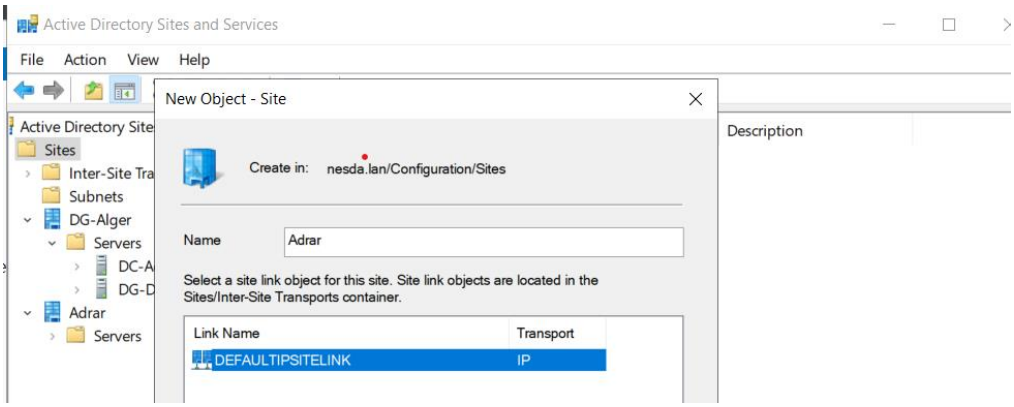

Figure III-28: création de site Adrar au DC01

- Puis la Création de "AD Subnets" pour les Sites Alger et Adrar :

  Tools → AD Sites and Services →Subnets → New Subnet .On doit attribuer les adresses ip au site correspondants, 10.10.3.0/24 au DG-Alger et 10.10.20.0/24 au Adrar

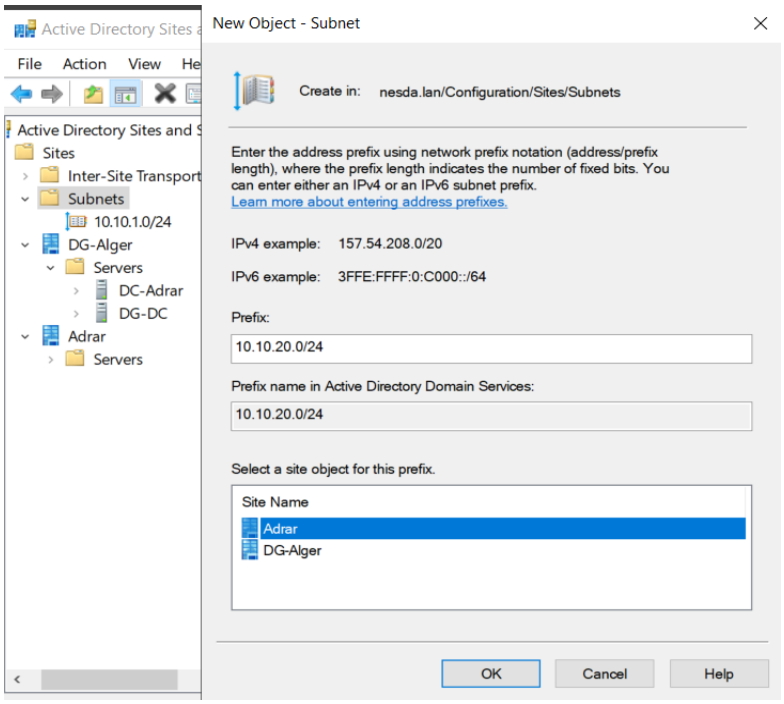

Figure III-29: Attribution des adresses ip pour les sites

- Après, on doit Déplacer chaque "DC" vers le Site approprié, DC01 à Alger et DC-Adrar vers le site Adrar

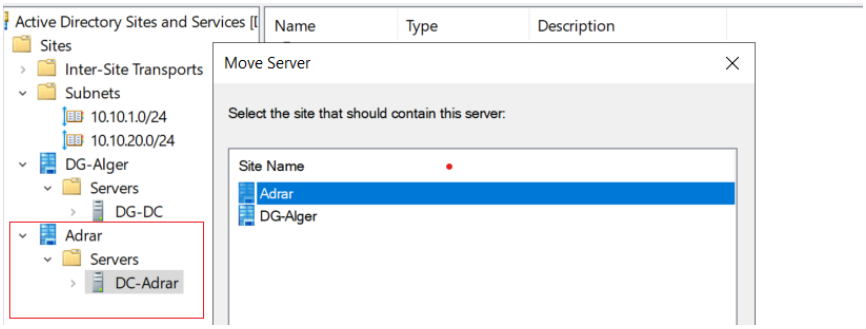

Figure III-30: déplacement des DCs vers les Sites

III.6.4.Ajout de " Site Link " entre les Sites Alger et Adrar

Nous avons connecté les deux sites avec un liens entre eux , Au sein de DCO1(Alger) :

Tools→ AD Sites and Services →Inter-Sites Transports → ip →new Site link

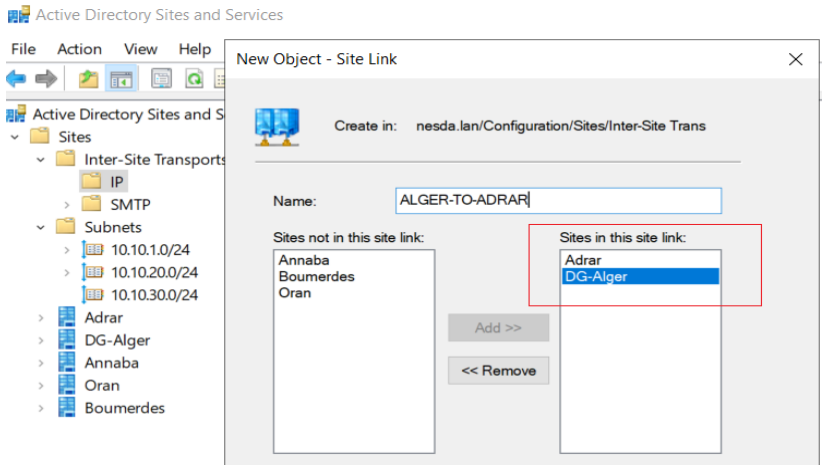

Figure III-31: création d'un lien entre Alger et Adrar

III.6.5.Activation de la Replication

La derniére étape consiste à activer la réplication sur les deux "Controlleur de domaine" DC01 et DC-Adrar.

AD Sites and Services→DG-Alger→DG-DC→Replicate Now

AD Sites and Services→Adrar→DC-Adrar→Replicate Now

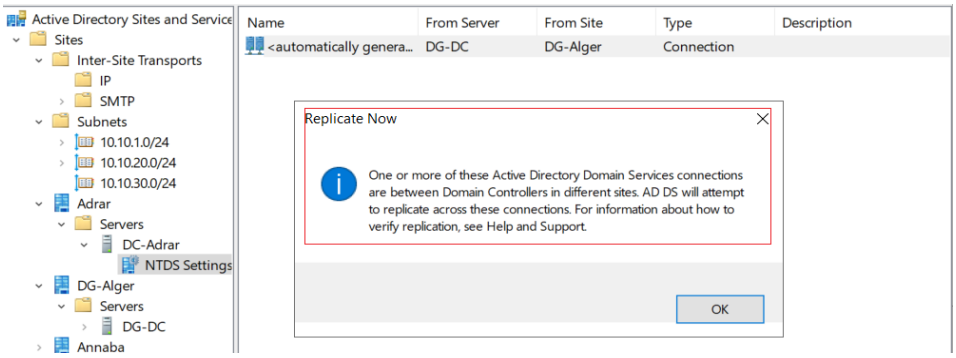

Figure III-32: Activation de la Réplication

Nous avons fait des échanges et modifications au sein du DC01(Alger) , puis nous avons constaté l'envoie des mises à jour avec succés vers la destination "DC-Adrar" :

DC01→Cmd→repadmin /showrepl

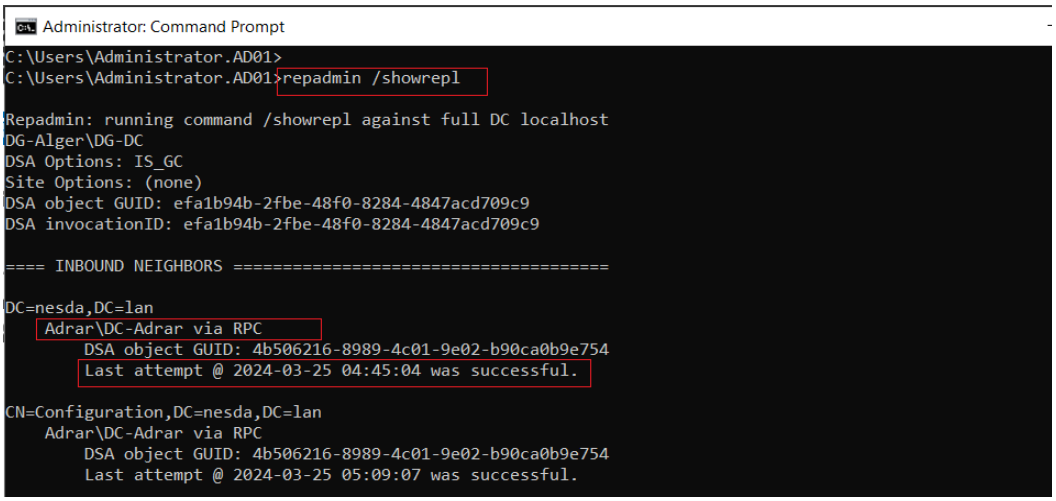

Figure III-33: teste de la replication

III.7.Configuration et Mise en Plaçe de Sécurité pour le DMZ

Nous somme basés dans le dévelopement de sécurité sur les principes de DMZ notamment :

Les requêtes depuis l'internet serons dirigées uniquement vers le DMZ et ne peuvent pas accéder au réseau privé (ex :DG-Local) , les serveurs de DMZ ne peuvent à aucun cas accéder aux réseaux privés ou publics , aussi le traffic généré au niveau des LANs est permis d'accéder au DMZ .

III.7.1. La Création d'une interface DMZ

Les Meilleures recommandations sont : définir une adresse ip statique et le rôle de l'interface sur DMZ et Désactiver tous les Accés administratifs (ping,telnet ,ssh …etc).

DG-FortiGate→Interfaces→Port3

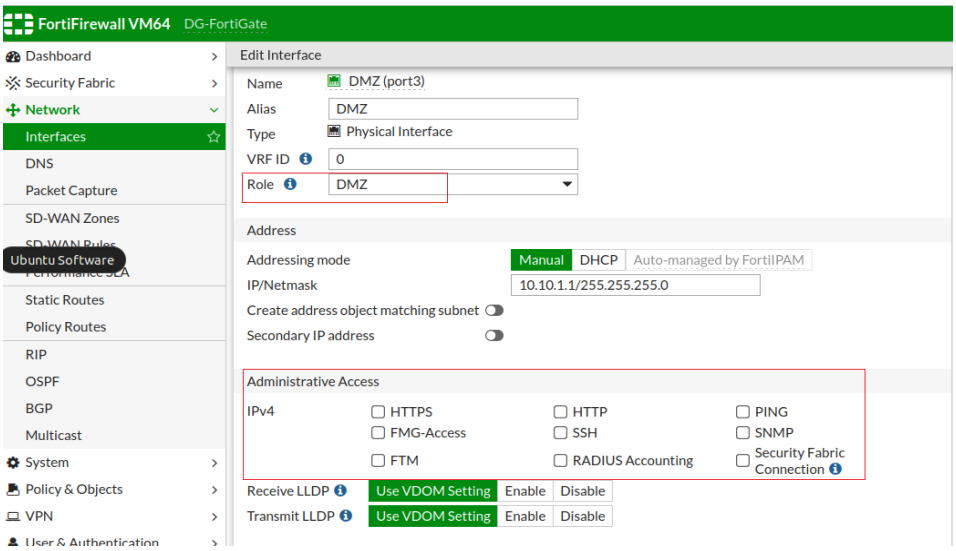

Figure III-34: L'ajoute de l'interface DMZ

III.7.2. La Mise en Plaçe de securité pour le Serveur Web Apache

Nous avons deux parties , la premiére pour le trafic externe et la seconde pour le trafics interne

III.7.2.1. Accés Externe à Partir d'un Réseau Public

Dans notre cas , port1 (DG-FortiGate) est considéré comme une interface publique avec l'adresse ip 192.168.1.7

- Au début, nous avons configuré le DNAT par la création de deux VIP (virtual ip) , pour que notre serveur web soit accéssible depuis l'internet.

  La premiére VIP est pour le protocol Https avec le port 443, et la deuxiéme pour http avec le port 80 : DG-FortiGate→Policy &Objects→Virtual ips

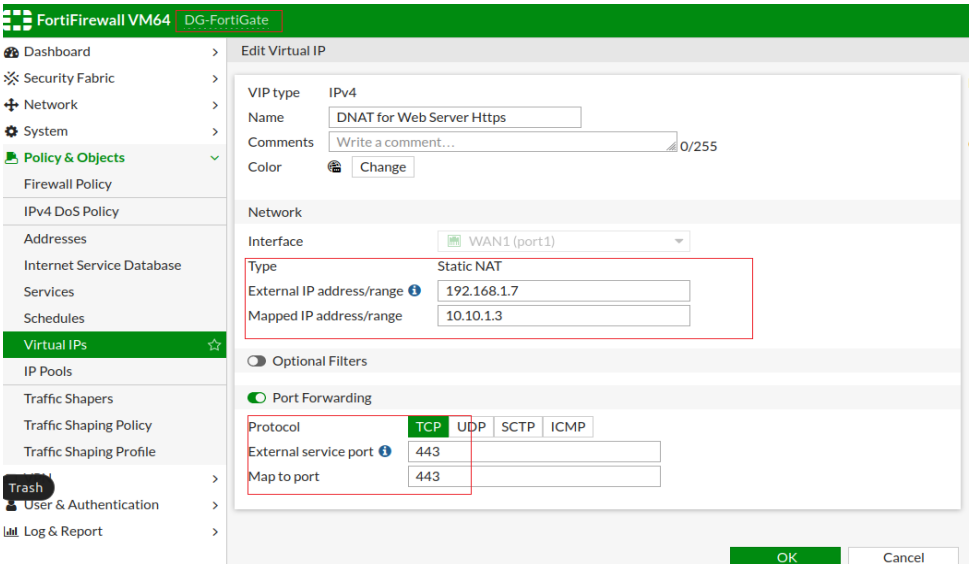

Figure III-35: la création d'une VIP pour Https

- Ensuite , nous avons bloqué "Web Application Attacks " en utilisant un WAF (Web Application Firewall) qui est un "reverse proxy" , pour protéger le serveur de certaines attaques telles: Sql injection , Credit Card detection , http flood …etc.

DG-FortiGate→Security Profiles→WAF→ Create new

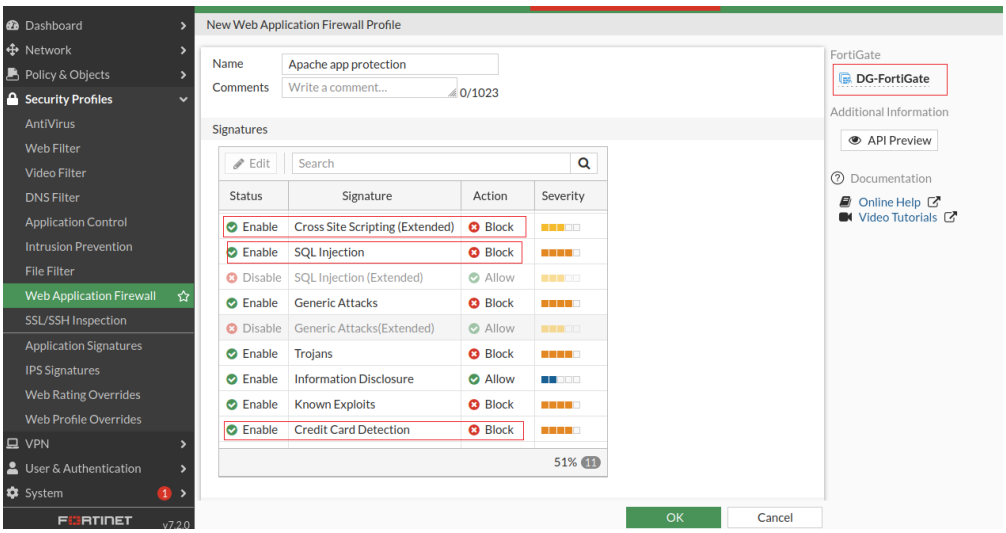

Figure III-36: Ajouter les Signatures de WAF

Aussi,activé les contraintes http pour la protection contre les différentes "attaques http" notamment : illegal http requeste methode , illegal http version …etc

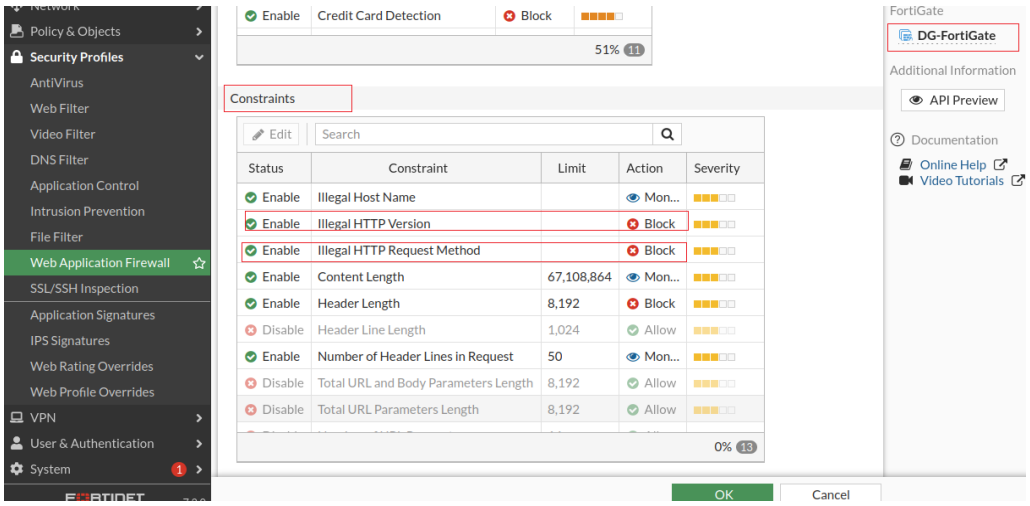

Figure III-37: Activation des Contraintes http

- Encore, nous avons ajouté un capture IPS , ce systéme de prévention contre les intrusion (Intrusion Prevention Sys) doit inspecter tous le trafic prevenant de l'internet aussi détecter et bloquer les activités malveillantes qui se cache dans ce traffic légitime .

  DG-FortiGate→security profile→Intrusion Prevention→Create new

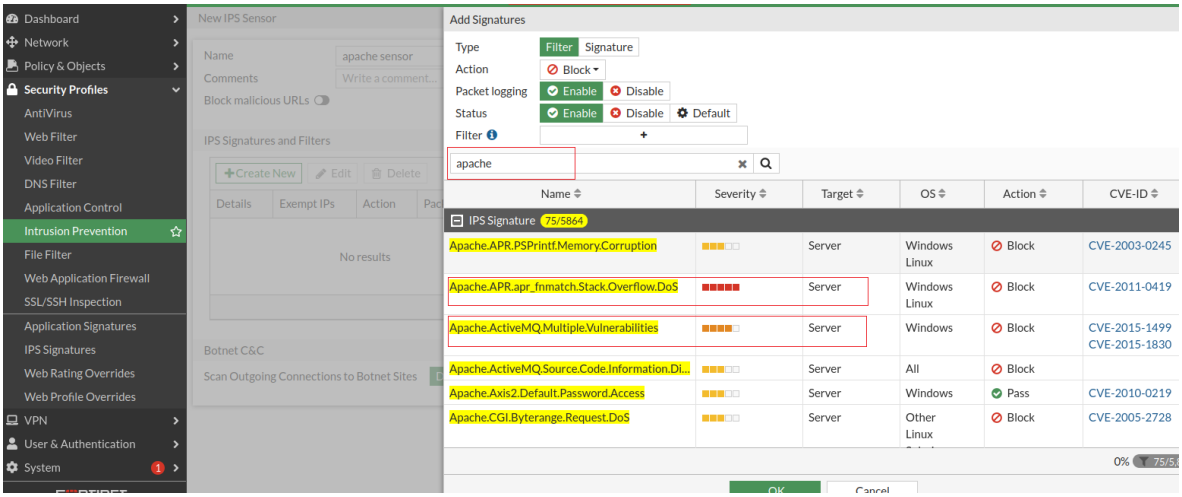

Figure III-38 :Ajout d'une Capture IPS

- Puis, nous avons rendu le serveur accéssible à partir d'internet par la création d'une nouvelle "Firewall Policy" qu'elle doit integrer le WAF, IPS .

On a utilisé les deux VIPs comme des adresses de Destination pour que le DNAT soit fonctionnel , puis désactivé le NAT et définir le mode d'inspection en "proxy based" et autoriser que les protocoles http et https .

DG-FortiGate→Policy&Object→Firewall policy

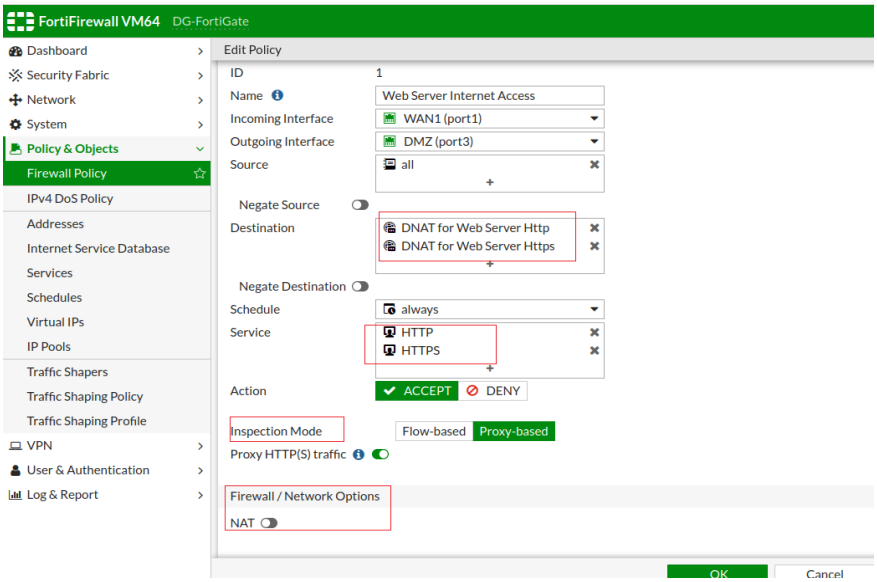

Figure III-39: création d'une politique pour le seveur web

- Teste depuis l'internet avec l'adresse public 192.168.1.7 sachant que l'adresse ip de notre serveur est 10.10.1.3 ce qui confirme la fonctionnalité de DNAT .

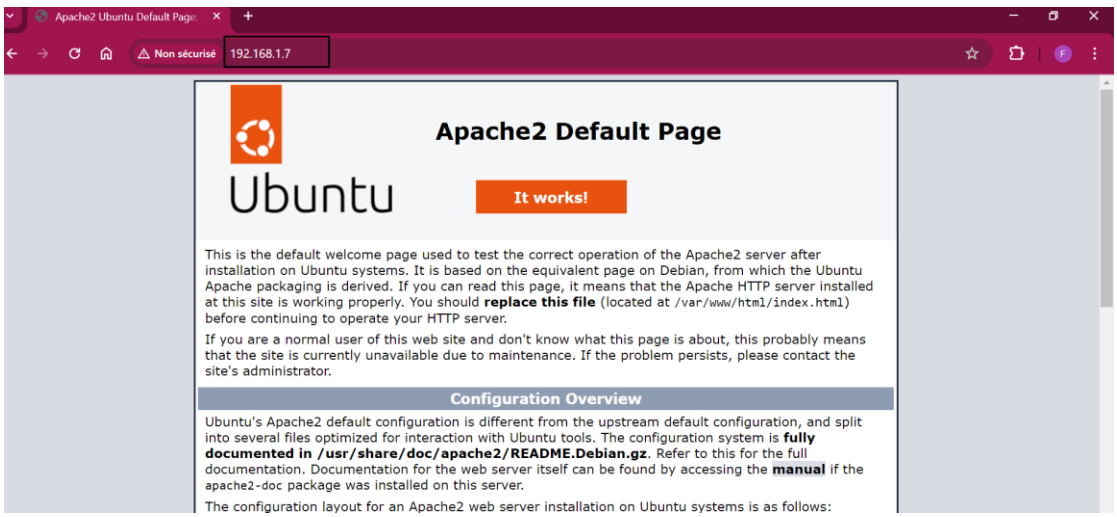

Figure III-40: L'accés au serveur web depuis l'inernet

- Ensuite, nous avons intégré sur l'interface publique une protection contre "DDos attack" et bloquer les botnet-sites par l'ajout d'une "DOS Policy' DG-FortiGate→Policy&Objects→ipv4 Dos policy

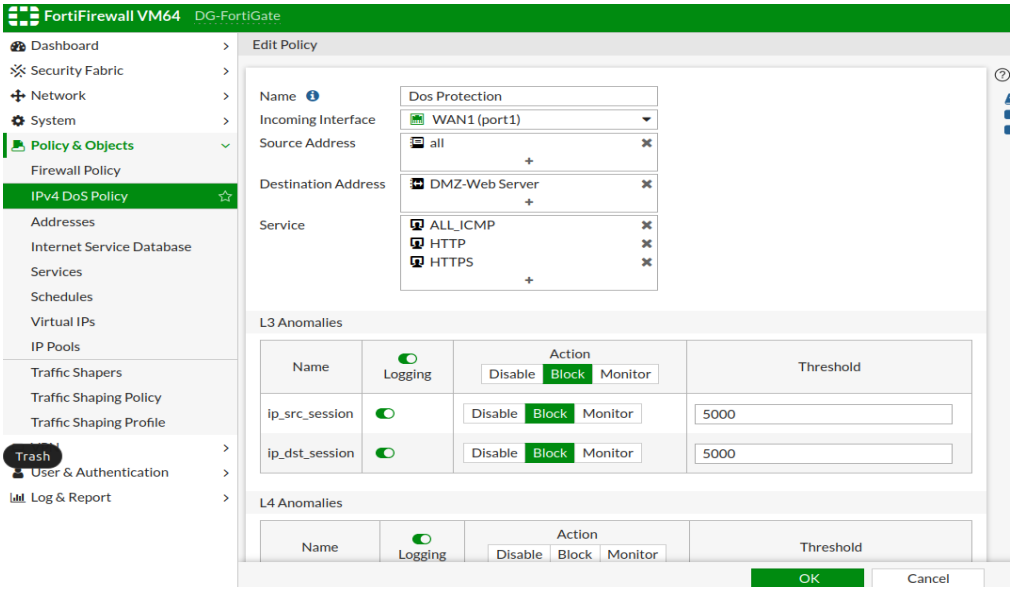

Figure III-41: l'integration d'une Dos Policy

- En dernier lieu, nous avons bloqué le trafic de "fichiers-compressés" (bzip,zip,rar…) d'étre téléchargés depuis l'internet par la création d'un nouveau "IPs Signature" : security profiles→IPS Sig→Create new

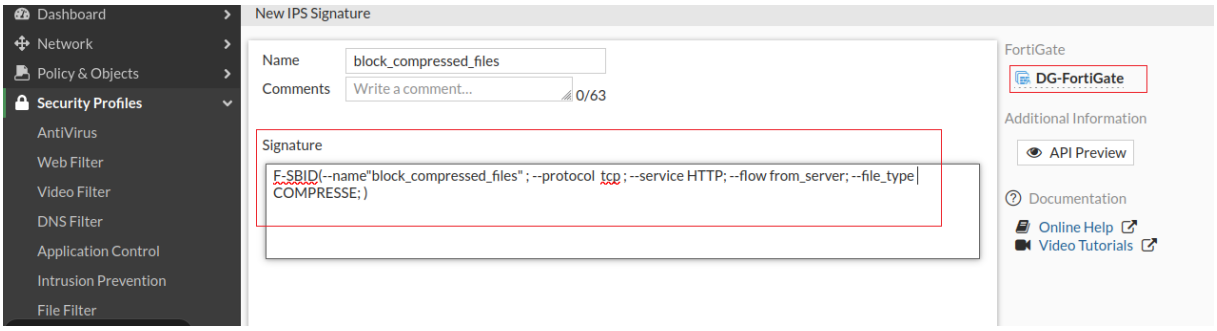

Figure III-42: La Création d'une nouvelle Signature IPs

Nous devons lier cette signature avec une capture IPs , puis intégrer cette dernier dans la politique(Firewall policy) qui autorise les employés d'accéder à internet.

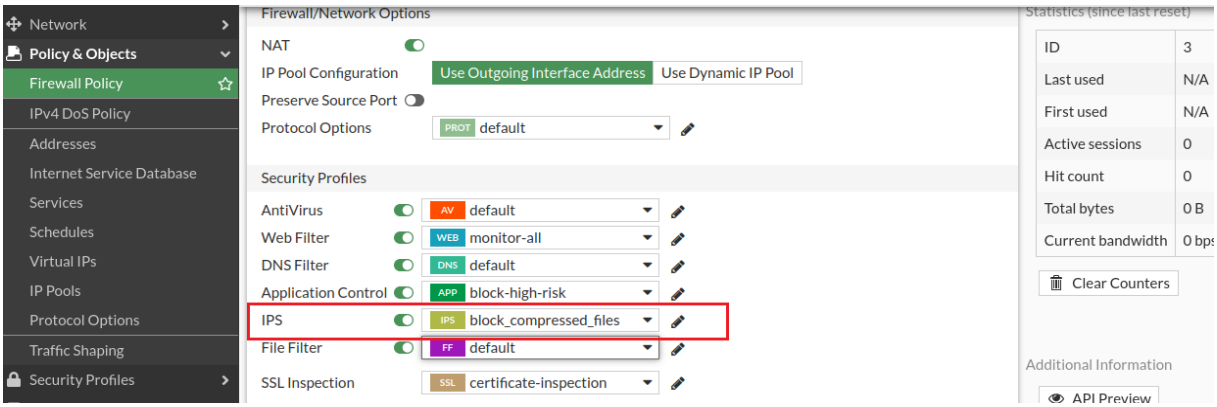

Figure III-43: Intégration de capture IPs avec la politique de sécurité

III.7.2.2. Accés Interne à Partir des Réseaux locaux

Au niveau de l'architecture , nos réseaux locaux tels que DG-local et Adrar-lan sont des réseaux fiables (trust networks).

Donc nous avons besoin de juste autorisé le trafics vers le serveur Web par la création des politiques de pare-feu , pour la manipulation on a utilisé le cas de réseau local : Adrar-lan.

- Sous DG-FortiGate

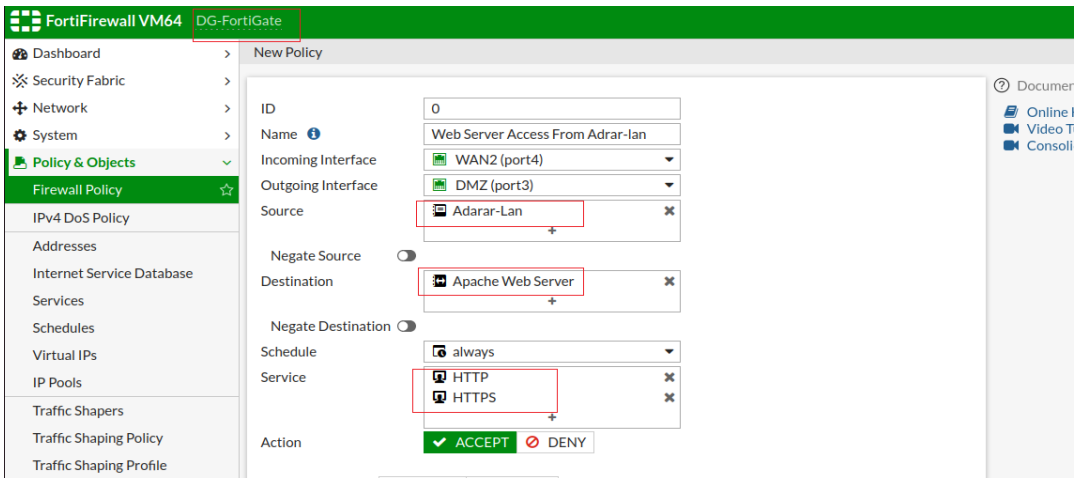

Figure III-44: Autorisation de traffic sous DG-FortiGate

- Sous Adrar-FortiGate

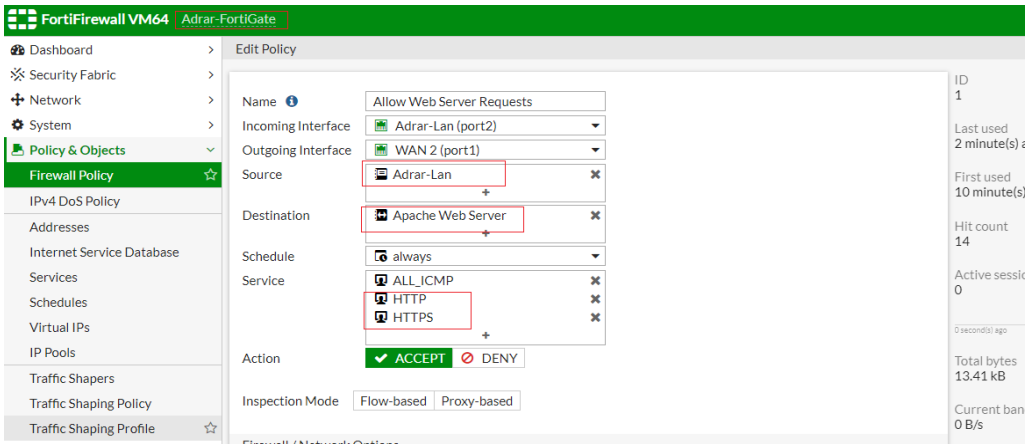

Figure III-45: Autorisation de trafic sous Adrar-FortiGate

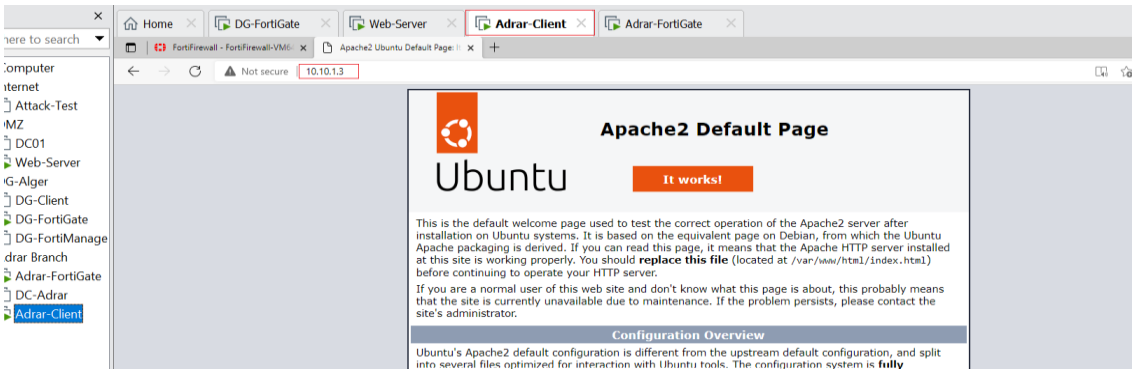

Figure III-46:Test depuis le reseau Adrar-lan

III.7.2.3.Tester La Securité Depuis L'inernet

- D'abord, sur la machine "Attack-Test" nous avons testé la couche 3 (Network) selon le modele OSI et la couche 4 (Transport) par les Attaques "icmp-Flood" et "Tcp-Scan-Port"

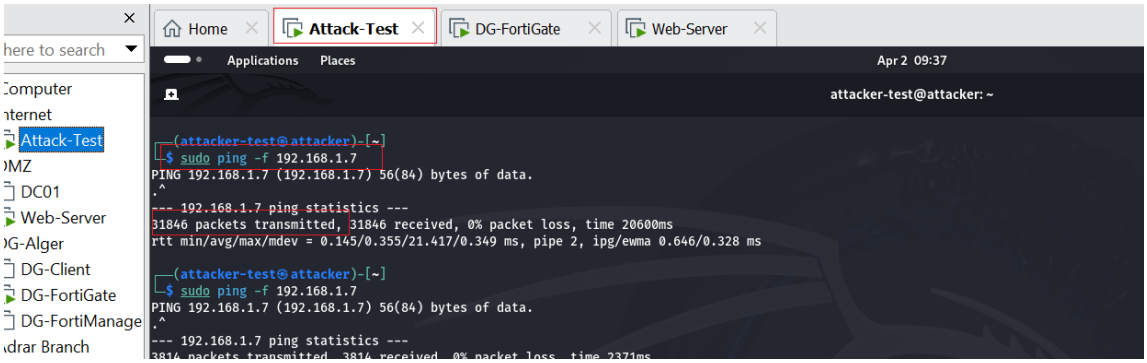

Figure III-47: l'attaque icmp-Flood

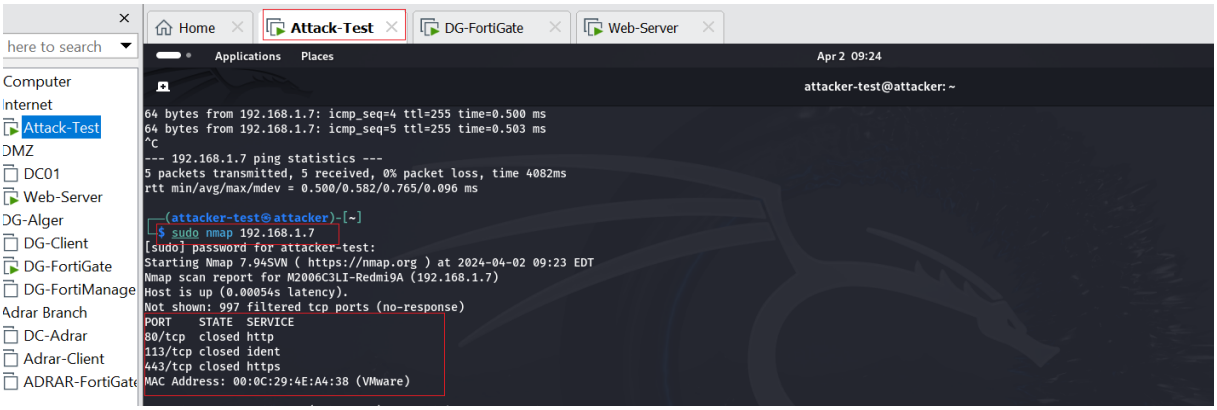

Figure III-48: l'attaque Tcp-Scan-Port

Sous DG-FortiGate, on a reçu des Alertes avec les noms d'attaques plus des informations sur le pirate.

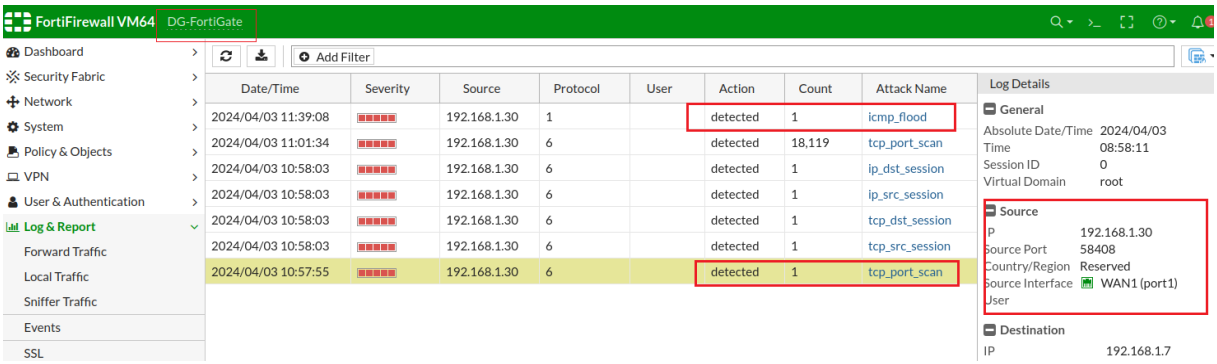

Figure III-49: les Alertes sur icmp-flood et Tcp-scan-port

- Ensuite , nous avons testé la couche application (couche 7) par l'attaque "http-Flood" en éxecutant un script python sur la machine attack-Test.

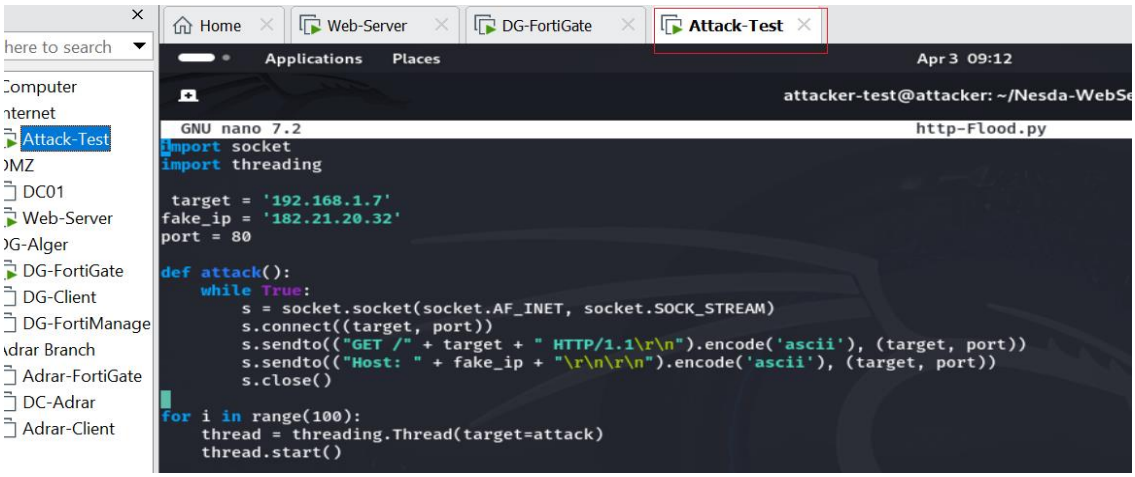

Figure III-50: le code python de l'attaque http-flood

Avant de déployer les exigences et les politiques de sécurité , nous avons reçu un nombre massive des requêtes sur le serveur environ 12769 requêtes (65.5 req /sec).

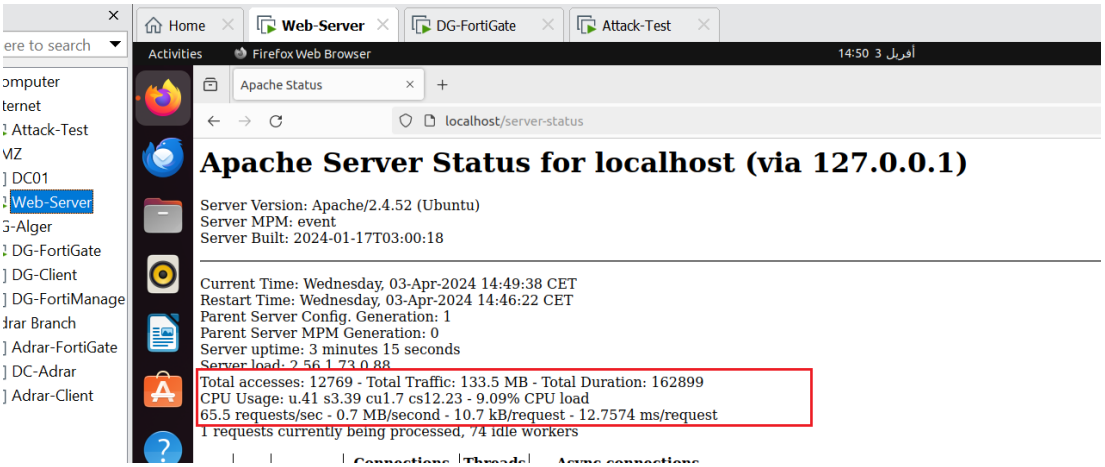

Figure III-51: l'effet d'attaque sur le serveur avant la protection

Mais après la protection avec les étapes qu'on a vu précédemment , l'attaque "http-Flood" a été bloquée au niveau de DG-FortiGate et n'a pas pu atteindre le serveur .

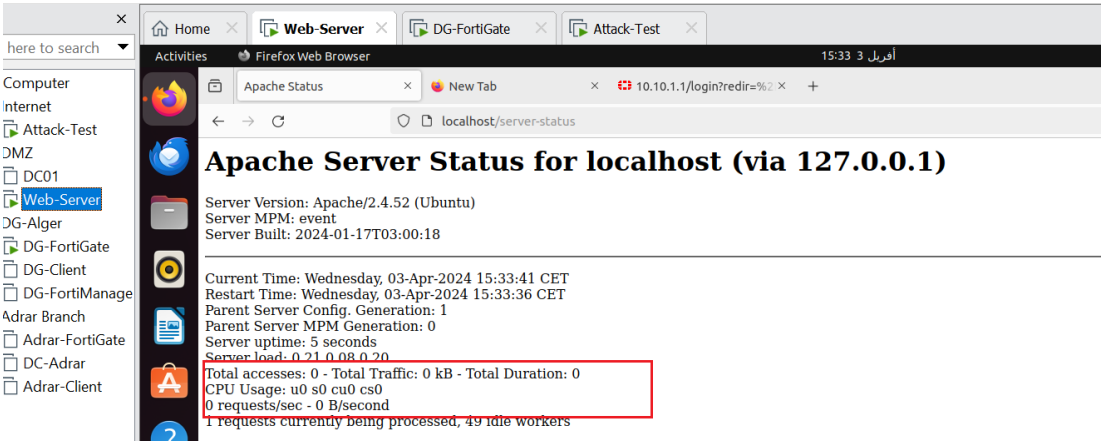

Figure III-52:Effet d'attaque sur le serveur aprés la protection

On nous référant aux résultats obtunus, nous avons confirmé la robustesse de notre sécurité .

III.8.Remote Access SSL-VPN

Nous avons employé " Mohamed Yassin " qui réside à Boumerdes et travaille à Nesda siege d'Alger, donc on doit lui fournir un accés a distance aux ressources internes(internal network) lorsqu'il est en dehors du siége Nesda par le ssl-vpn .

III.8.1. Authentification à distance(remote authentication)

Pour l'athentification vpn , il est difficile de gérer et manipuler tous les utilisateurs (employés) et leurs passwords si nous utilisons "local authentication" sur DG-FortiGate.

Pour cela,nous avons pris l'avantage du protocole LDAP pour relier DG-Fortigate avec AD DS qui doit fournir les services d'authentification et récupération d'informations d'identification.

III.8.1.1. La Configuration de LDAP (Lightweight Directory Access Protocol)

L'objectif est de définir la machine DG-FortiGate comme "LDAP Client" et DC01 comme un "LDAP Server" .

- Tout d'abord, l'ulilisateur "Mohamed Yassin" est enregistré au ADDS (DC01) ,on note qu' il appartient au groupe "Comptabilité/Boumerdes remote access"

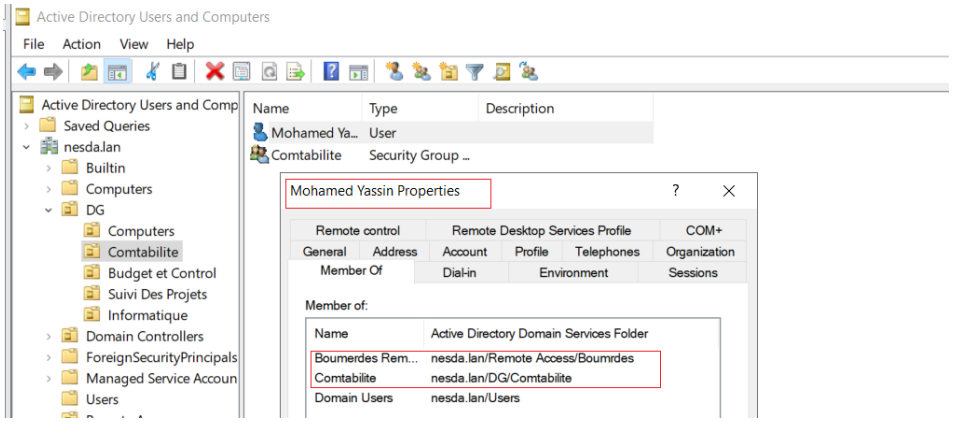

Figure III-53: les proprietés de mohamed yassin

- Ensuite,nous avons défini le rapport entre DC01 et DG-FortiGate :

Users&authen→LDAP servers→Create new

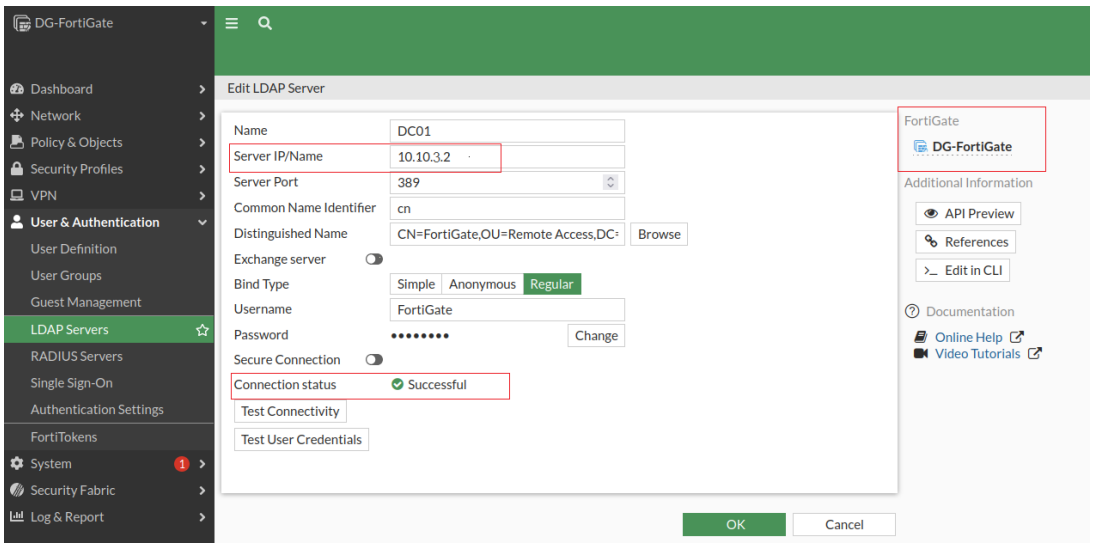

Figure III-54: configuration de relation entre DC01 et DG-FortiGate

- Puis, nous avons créé un groupe d'utilisateur sur DG-FortiGate et choisi depuis ADDS le groupe "boumerdes Remote Access" :User&authen→user Group→Create new

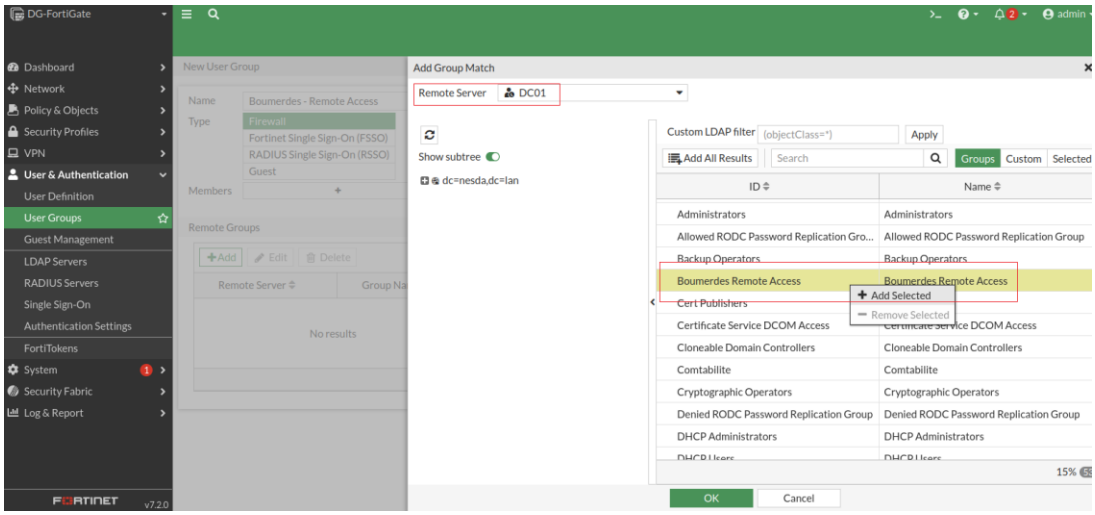

Figure III-55: La Création de nouveau Groupe

III.8.2.La Configuration du SSL-VPN

Nous devons créer un portail VPN SSL pour y affecter notre groupe, pour donner accès uniquement au réseau "internal ressources" et définir certaines autorisations et privilèges.

Puis, nous avons défini le mode Tunnling pour n'autoriser que le trafic client dans lequel la destination correspond à la destination configurée :VPN→SSL-VPN Portals→Create new

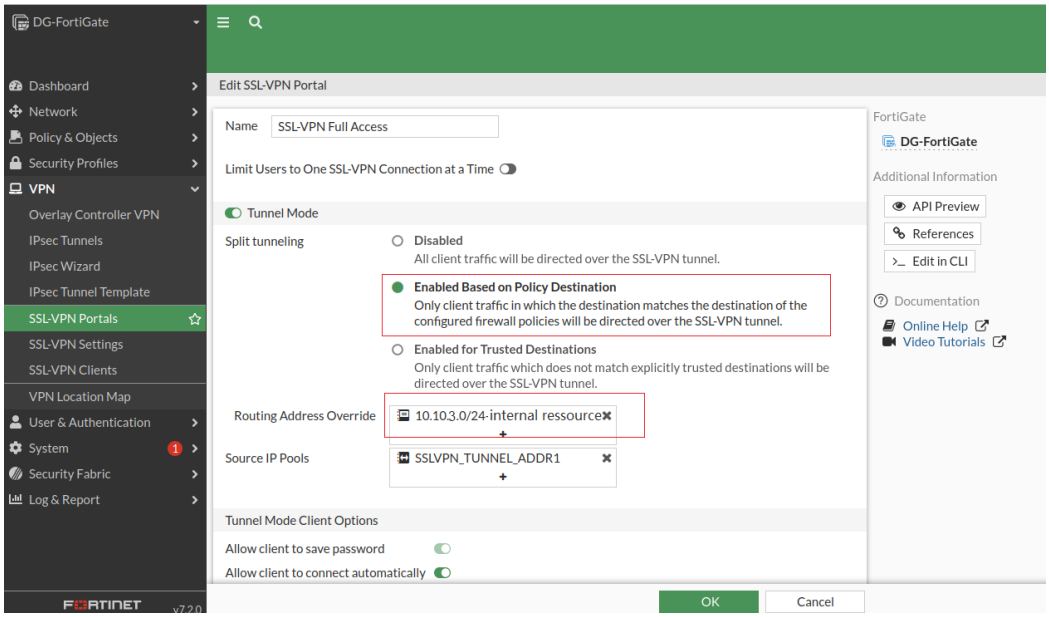

Figure III-56: la création de portail ssl-vpn

Ensuite,nous avons configuré les paramétres de ssl-vpn en choisissons l'interface WAN1(port1) comme une interface d'écoute, aussi les utilisateurs seront automatiquements déconnectés s'ils n'ont pas d'activités pendant 5 min, Nous devons changer le port ssl par défaut 443 en 10443 pour éviter les conflits de ports avec HTTPS : VPN→SSL-VPN Settings

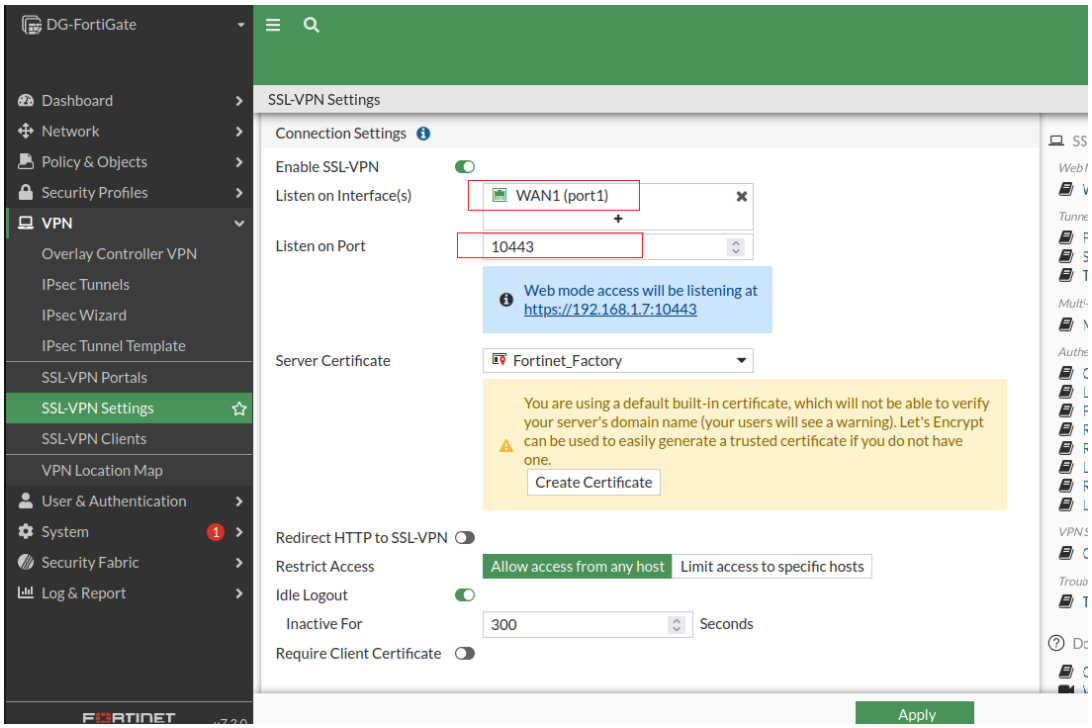

Figure III-57: les parametres de ssl-vpn

De plus, Nous avons fait correspondre le portail (ssl-vpn full access) que nous avons créé, avec le groupe "Boumerdes Remote Access"

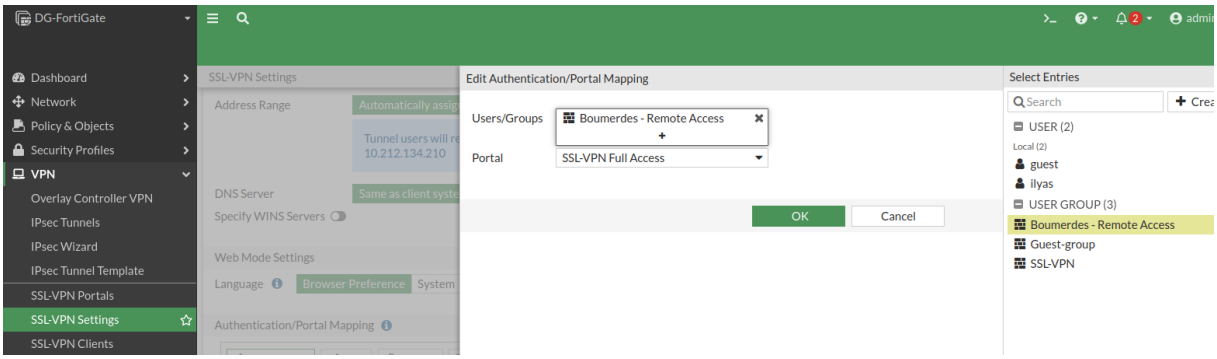

Figure III-58: liaison de portail avec le groupe correspondant

Finalement,nous avons créé une politique ssl-vpn pour permettre le trafic, on note que l'interface entrante sera l'interface logique "SSL-VPN tunnel int" créé par défaut, aussi nous avons également spécifié le groupe dans le champ source.

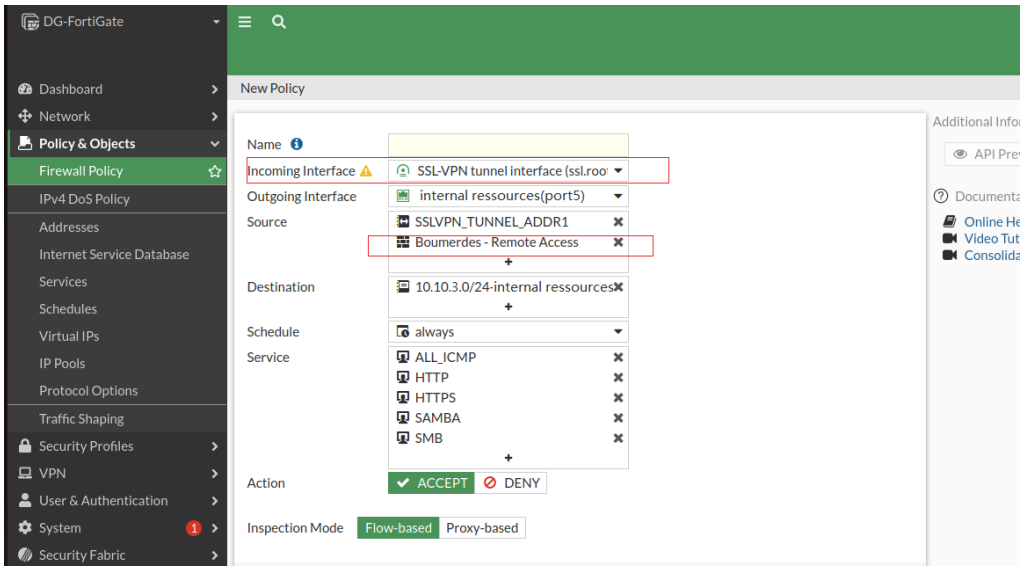

Figure III-59: la création d'une politique pour ssl-vpn

III.8.3. Accés à Distance Depuis Le Site De Boumerdes

Parce que nous utilisons "Tunnel mode" et pas le Web mode ,au niveau de la machine "Remote User" nous avons installé le logiciel (software) "FortiClient" teléchagé à partir [W26] .

Donc ,après avoir entrer au FortiClient et localisé le champ "remote access" , nous avons choissi ssl-vpn et spécifié l'adresse ip 192.168.1.7 de l'interface public WAN1(port1) de DG-FortiGate , ensuite taper les information de l'identification (credentials) de l'émployé.

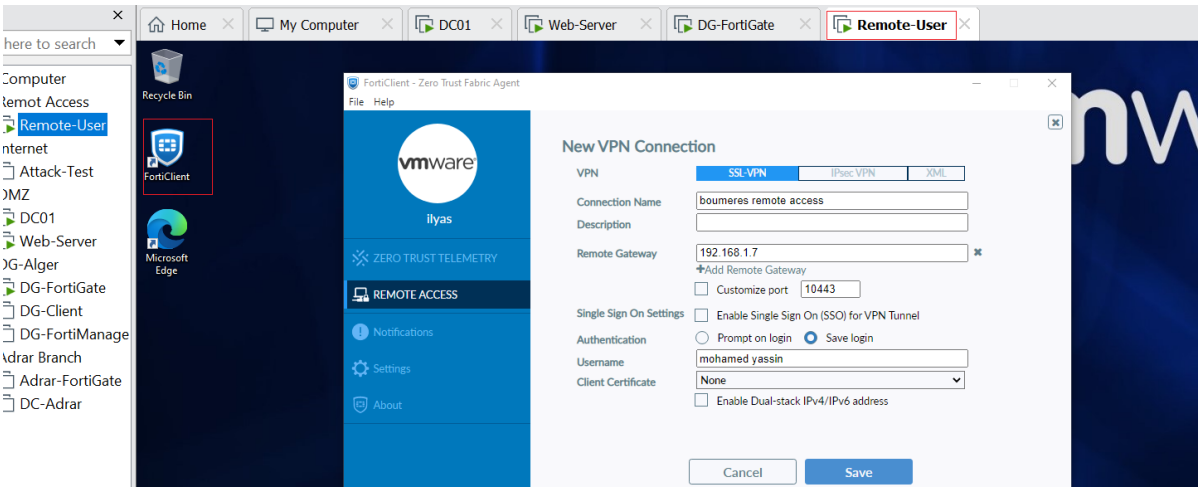

Figure III-60: Accés par l'outile FortiClient

.

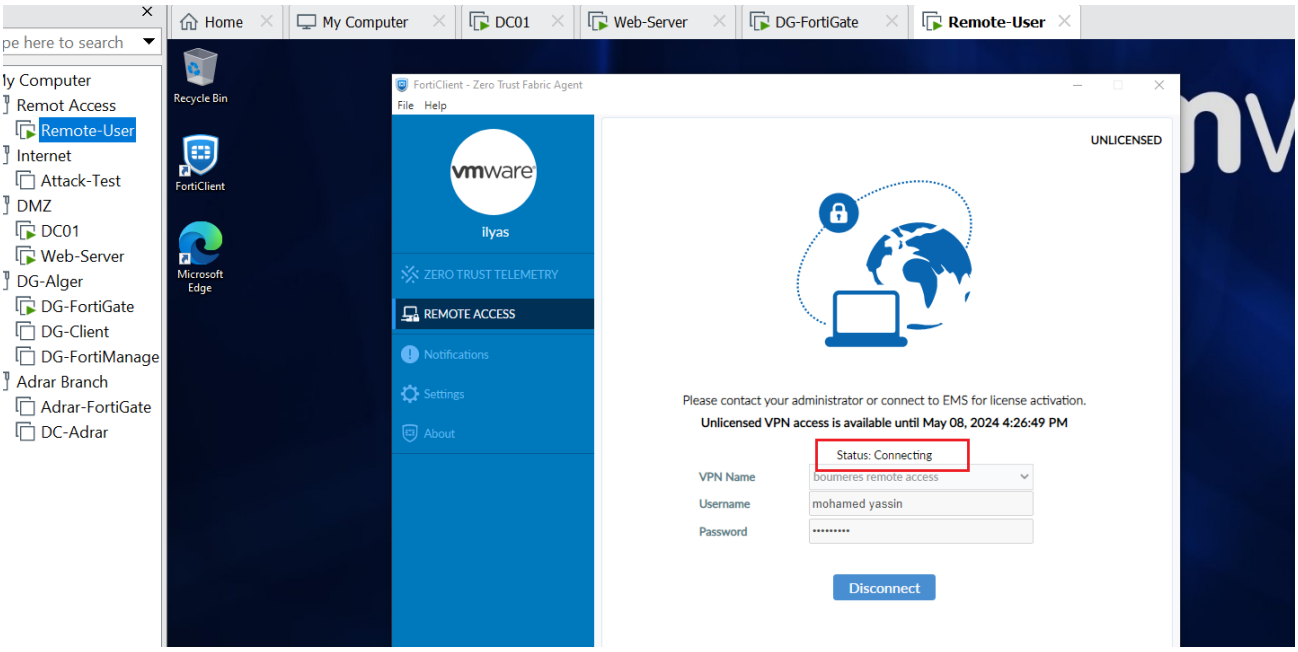

Figure III-61: la réussite de connection vpn

Après avoir l'opération sera términée avec succés, nous pouvons maintenant accéder au réseau interne (Internal ressources) et plus précisement au serveur de fichier, et grace à ce VPN l'employé "Mohamed Yassin" a pu consulter ces fichiers correspondants en sécurité total .

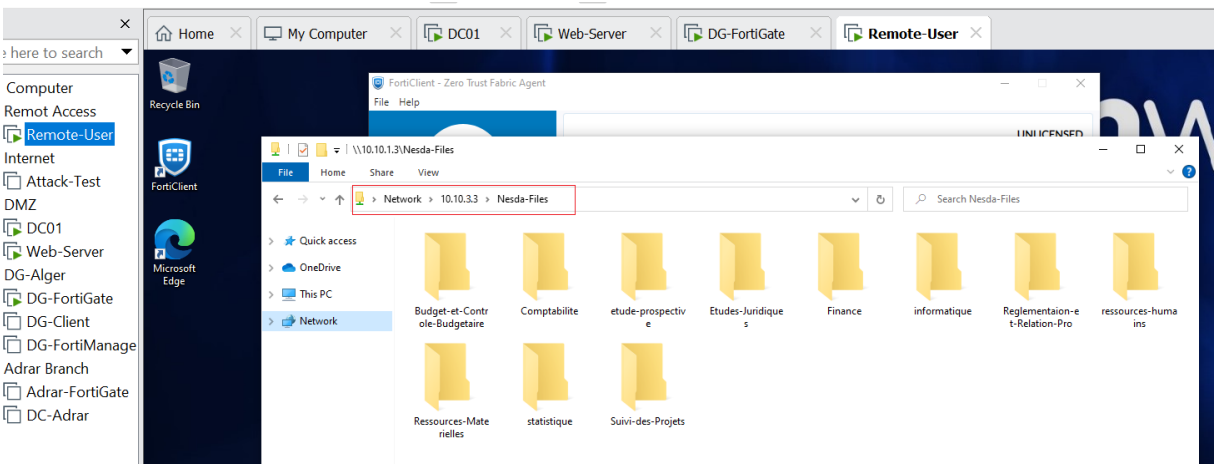

Figure III-62: Accés aux ressources interne

III.9. Conclusion

La sécurité d'un réseau est extrêmement importante au sien d'une entreprise. C'est pourquoi, la mise en place de solutions de protection, de surveillances telles qu'un firewall permet de répondre à ce besoin de sécurisation.Dans ce chapitre,nous avons répondu aux besoins de l'entreprise Nesda et réalisé les solutions proposées qui nous ont permis de renforcer notre politique de sécurité.

Conclusion générale

L'objectif principal de notre projet de fin d'étude était de répondre aux besoins spécifiques de l'entreprise en matière de sécurité informatique. En développant une solution sur mesure basée sur le pare-feu de nouvelle génération "FortiGate" , nous avons pu aider l'entreprise à renforcer leur sécurité et améliorer les performances globale de leur réseau en termes de Fournir un accés à distance "sécurisé" et peu coûteuse au ressources internes,la Création d'une zone démilitarisée DMZ avec implémentation des règles de sécurité correspondantes, amélioration de la vitesse et simplifier l'administration en créant un réseau pour les ressources internes ,Optimisation de trafic WAN et la protection contre les attaques online en intégrant des stratégies de firewall , un système de prevention des intrusion, une politique DoS et un WAF (Web application Firewall).

Dans un premier temps, nous avons présenté les concepts fondamentaux des réseaux informatique, dans lequel nous avons fait un petit aperçu sur les architectures , les différents services plus des notions sur Active Directory Domain services. La deuxiéme partie de ce chapitre , consiste à une introduction sur la sécurité informatique, nous avons mis un accent sur les termes et les méthodes de sécurité de données avec une explication sur les réseaux DMZ.

Ensuite, une étude sur la sécurité informatique nous a permis d'exposer un large panorama sur les différentes attaques qui peuvent affecter notre réseau et leurs types, sans oublier les politiques de sécurité et la gestion des risque qui entoure l'entreprise.Puis, nous avons bien détaillé les solutions disponible de la sécurité, en présentant les pare-feu et leurs fonctionnement, les proxy, les systémes de prévention d'intrusions,les WAF,les politique de DoS et les réseaux privés virtuels.

En effet, la mise en place des régles de firewall avec la création des nouveaux réseaux et l'implementation d'un systéme de prévention d'intrusion, une pilitique DoS, un VPN et les autres solutions proposées ont permis d'assurer et renforcer la sécurité informatique du réseau NESDA

Ce projet nous a permis d'acquérir une expérience personnelle et professionnelle et ne peut être que bénéfique. Ce fut une occasion pour se familiariser avec l'environnement du travail et de la vie professionnelle ainsi que d'élargir et d'approfondir nos connaissances sur l'administration et la sécurité des réseaux informatiques. En termes de perspectives; nous pouvons intégrer le dispositif " Email Security appliance " (ex : ESA Cisco) pour protéger les

employés et le réseau NESDA en général contre les attaques basées sur les emails notamment le phising ;les spam …etc.

Bibliographie

[1] Med Amine Riahla,"Polycop sur les réseaux informatiques",Universite M'hammed bouguerra Boumerdes,2016

[2] Cricket Liu, Paul Albitz.« DNS and BIND », United States of America. O'Reilly Media.ISBN: 9780596100575,may 2006

[3] Allied Telesis.«Dynamic Host Configuration Protocol - DHCP.Feature Overview and Configuration Guide » Bothell,USA.2022

[4] IBM Corp.« System i: Networking Domain Name System »,Version 6 Release 1.2008

[5] William R,Stanek . «Active Directory Administration:The Personal Trainer » United States of America,2015

[6] Brian Desmond, Joe Richards, Robbie Allen, and Alistair G. Lowe-Norris.« Active Directory »,United States of America. O'Reilly Media.ISBN:978-1-449-32002-7. april 2013

[7] Steve Clines,Marcia Loughry. « Active Directory® For Dummies,® 2nd Edition »,Wiley Publishing, Inc., Indianapolis, Indiana.2008

[8] Alan Calder.«Cyber Security,Essential principles to secure your organisation »IT Governance Publishing Ltd.Cambridgeshire,United Kingdom.ISBN 978-1-78778-210-5,2020

[9] Awadhesh Kumar Maurya,Mudassir Khan,Neeraj Kumar.«Cyber Security » Nitya, Bhopal MP India.ISBN : 978-93-90178-78-0, 2020

[10] Livret enseignant.« Former à la cybersécurité » l'Agence nationale de la sécurité des systèmes d'information et le ministère de l'Éducation nationale et de la Jeunesse,

[11] Trend Micro.« Sécurité informatique POUR LES NULS™ EDITION PME-PMI »John Wiley & Sons, Ltd.West Sussex,Angleterre.ISBN : 978-0-470-66694-4,2010

[12] John R, Vacca.«CYBER SECURITY AND IT INFRASTRUCTURE PROTECTION » Steven Elliot.Waltham, USA.ISBN: 978-0-12-416681-3,2014

[13] Cisco CCNA3,Module 3 « Network Security Concepts» Enterprise Networking , Security, and Automation v7.0.

[14] iCIMS.«Policy Document»,Policy Version 2.3, Date: 8/23/2022

[15] SANS Institute.«Server Security Policy», October 2022

[16] SANS Institute.«Remote Access Policy», October 2022

[17] SANS Institute.«Email Policy», Dec 2013

[18] Pedro Ramos Brandao.José Almeida« Next-Generation Firewalls: Concept, Features, and Their Benefits»,Edition No. 9 – 11-10-2021

[19] sonicwall.«DataSheet-Email Security Apps And Software»,USA,2021

[20] Cisco CCNA2,Module 10 «LAN Security Concepts»Switching, Routing and Wireless Essentials v7.0 (SRWE)

[21] A.Shaji George, A.S.Hovan George.«A Brief Study on The Evolution of Next Generation Firewall and Web Application Firewall»,International Journal of Advanced Research in Computer and Communication Engineering,May 2021

[22] Cisco CCNA3,Module 8 « VPN and IPsec Concepts» Enterprise Networking , Security, and Automation v7.0.

Webographie

[W1] https://homepages.laas.fr/adoncesc/STAPS/Informatique/Introductionreseaux1-2.pdf ,consulté le 21/04/2024.

[W2] https://sti.ac-versailles.fr/IMG/pdf/reseau.pdf

[W3] https://www.techtarget.com/searchnetworking/definition/file-server ,consulté le 23/04/2024.

[W4] https://developer.mozilla.org/en-US/docs/Learn/Common_questions/Web_mechanics/What_is_a_web_server ,consulté le 23/04/2024.

[W5] https://www.quest.com/learn/what-is-a-domain-controller.aspx#:~:text=A%20domain%20controller%20(DC)%20is,AD%20DS)%20installed%20on%20it. ,consulté le 24/04/2024.

[W6] https://www.fortinet.com/fr/resources/cyberglossary/what-is-dmz ,consulté le 28/04/2024.

[W7] https://www.fortinet.com/fr/resources/cyberglossary/eavesdropping ,consulté le 06/05/2024.

[W8] https://www.geeksforgeeks.org/active-and-passive-attacks-in-information-security/ ,consulté le 06/05/2024.

[W9] https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-ip-address-spoofing-attack#:~:text=IP%20spoofing%20is%20a%20malicious,system%20or%20hide%20their%20identity. ,consulté le 06/05/2024.

[W10] https://www.fortinet.com/resources/cyberglossary/computer-virus#:~:text=Computer%20Virus%20Definition&text=A%20computer%20virus%20is%20a,in%20data%20loss%20and%20leakage. ,consulté le 06/05/2024.

[W11] https://orbit-computer-networking.com/blog/understanding-network-trust-exploitation-attack ,consulté le 06/05/2024.

[W12] https://www.techtarget.com/iotagenda/definition/man-in-the-middle-attack-MitM ,consulté le 06/05/2024.

[W13] https://www.cloudflare.com/fr-fr/learning/ddos/what-is-a-ddos-attack ,consulté le 06/05/2024.

[W14] https://www.ibm.com/topics/cyber-risk-management#:~:text=IBM-,What%20is%20cyber%20risk%20management%3F,broader%20enterprise%20risk%20management%20efforts. ,consulté le 12/05/2024.

[W15] https://www.fortinet.com/resources/cyberglossary/proxy-server ,consulté le 12/05/2024.

[W16] https://www.esecurityplanet.com/networks/firewall-policy/#:~:text=A%20firewall%20policy%20is%20a,guard%20against%20potential%20security%20threats. ,consulté le 13/05/2024.

[W17] https://docs.fortinet.com/document/fortigate/7.4.3/administration-guide/771644/dos-policy ,consulté le 13/05/2024.

[W18] https://www.coursera.org/learn/advanced-network-security-first-course-1/lecture/zqCPJ/defining-instrusion-prevention-systems-and-how-intrusion-prevention-systems ,consulté le 14/05/2024.

[W19] https://getintopc.com/softwares/virtualization/vmware-workstation-pro-2023-free-download/ ,consulté le 27/03/2024.

[W20] https://www.nexigen.com/cyber-security/fortinet-fortigate-firewalls-everything-you-need-to-know/ ,consulté le 27/03/2024.

[W21] https://www.hostinger.com/tutorials/what-is-apache ,consulté le 27/03/2024.

[W22] https://httpd.apache.org/ ,consulté le 27/03/2024.

[W23] https://learn.microsoft.com/en-us/windows-server/administration/overview ,consulté le 27/03/2024.

[W24]https://www.redhat.com/sysadmin/getting-started-samba ,consulté le 31/03/2024.

[w25]https://www.ionos.com/digitalguide/server/configuration/samba-server-the-cross-platform-network/ ,consulté le 31/03/2024.

[W26] https://www.fortinet.com/support/product-downloads ,consulté le 13/04/2024.

[W27]https://www.wallstreetmojo.com/peer-to-peer/ ,consulté le 21/04/2024

[W28]https://www.geeksforgeeks.org/three-tier-client-server-architecture-in-distributed-system/ ,consulté le 21/04/2024

[W29] https://upload.wikimedia.org/wikipedia/commons/c/c9/Client-server-model.svg ,consulté le 21/04/2024

[W30] https://www.ibm.com/docs/en/ssw_ibm_i_71/rzakg/rzakg.pdf ,consulté le 23/04/2024

[W31] https://servermall.com/blog/best-server-for-file-server/ ,consulté le 23/04/2024

[W32] https://www.fiverr.com/agha_danish/install-configure-your-active-directory-domain-controller ,consulté le 29/04/2024

[W33] https://www.wallarm.com/what/cia-triad-definition ,consulté le 27/04/2024

[W34] https://daynhauhoc.s3.dualstack.ap-southeast-1.amazonaws.com/optimized/3X/4/d/4d24eb6fc59ac5eb638cab3a338585bcd4f0f201_2_690x413.png ,consulté le 12/05/2024