Mémoire de Master

Présenté au

Département : Génie Électrique
Domaine : Sciences et Technologies
Filière : Télécommunications / Electromécanique
Spécialité : Systèmes des Télécommunications

Réalisé par :

NAMAOUI Hocine Ramzi

Et

HAMITOUCHE Toufik

Thème

Sécurité des Réseaux et Firewalls

Soutenu le: **06/11/2021**

Devant la commission composée de :

Mr :	……	Prof.	Univ. Bouira	Président
	…… Rapporteur	M.C.A	Univ. Bouira	
	…….. Examinateur	M.C.B	Univ. Bouira	
	…….. Examinateur	M.A.A	Univ. Bouira	

Dédicaces 1

Avant tout, nous remercions ALLAH, le miséricordieux pour nous avoir donné la force, la patiente etla volonté afin de réaliser ce travail que je le dédie en signe de respect, reconnaissance et d'amour profond :

A mes chers parents ;

Aucune dédicace ne saurait exprimer mon ésprit, mon amour éternel et ma considération pour les sacrifices que vous avez consenti pour mon instruction et mon bien être.

A mes chères sœurs ;

A ma chère grande-mère, mes chers oncles et mes chères tantes ;

A toute la famille NAMAOUI ;

A toute la famille BOUCHELAGHEM ;

A mon binôme Toufik, qui a partagé ce travail avec moi ;

Mes remerciments vont à mes amis, particulièrement Manel, Amel et Mounia la directrice, et à tous ceux qui ont participé à l'élaboration de ce modeste travail et à tous ceux qui nous sont chers.

Dédicaces 2

Je tiens à la fin de ce travail à remercier ALLAH le tout puissant de m 'avoir donné la foiet de m'avoir permis den arriver là.

Je dédie ce travail à :

Ma très chère et douce mère L'étoile de ma vie qui fait briller mes jours les plus sombres,qui réchauffe mon cœur , tu es l 'amour àl 'état brut

A mon cher pére tu as assumé ton role de pére avec tendresse et fermeté Je pouvais pas avoir de m eilleure pére que toi .

A mes fréres : Aymen , Badro ,Ali ,A amira et son mari hocine et à la petite chamesse et a toute les familles HAMITOUCHE ,CHARCHER et YAKHLEF

Sans oublier l'équipe : Dinner time, spootted univ bouira ,fantasy family A mon **binome hocine** et tout sa famille , et les amis (Sido , Rezki ,Mohamed,Fares ,Aymen ,Manalo, Assia , kamel ,Farouk,Oussama,Modira,Achwak,Zahou)

Remerciements

Ce travail a été effectué au sein du Département des Sciences et sciences appliquées de l'Université de Bouira.

Je tiens à remercier, en premier lieu, Dr. MEDJEDOUB Smail, Directeur de ce mémoire pour ses conseils et son aide.

Nous tenons à montrer toute notre gratitude à nos deux encadreurs Mr. DOUKARI Samir et Mr. OUCHENE Mohamed, en les remerciant pour leur temps, leurs conseils, leur implication, leur disponibilité et gentillesse, et toute l'aide qu'ils nous ont apporté pour mener à bien la réalisation de ce travail.

Aussi, un grand merci pour le directeur d'Algérie Télécom Satellite, Mr. MAHMOUDI Azeddine, qui nous a donné cette opportunité de travailler au sein de la base d'ATS de «LAKHDARIA», ainsi que les moyens qu'il a mis à notre disposition.

Je remercie également tous les membres du jury pour l'intérêt qu'ils ont porté à mon travail :

Prof. Aissouni Salim …….

Dr. ……..

Mr.……..

Dr.……..

……..
……
……..

Enfin, j'associe à ces remerciements tous ceux qui ont contribué à réaliser ce travail.

Résumé

La **sécurité des réseaux** est devenue plus importante pour les les utilisateurs d'ordinateurs, les organisations et les militaires. Avec l'avènement d'Internet, la sécurité est devenue une préoccupation majeure. L'histoire de la sécurité permet de mieux comprendre l'urgence des technologies de sécurité. La structure d'Internet elle-même a permis l'apparition de nombreuses menaces pour la sécurité. L'architecture de l'internet, lorsqu'elle est modifiée, peut réduire les attaques possibles qui peuvent être envoyées sur le réseau. En connaissant les méthodes d'attaque, il est possible de mettre en place une sécurité appropriée. De nombreuses entreprises se protègent d'Internet au moyen de **firewalls** et de mécanismes de **cryptage**. Les entreprises créent un "**intranet**" pour rester connectées à l'Internet mais protégées des menaces éventuelles. Le domaine de la sécurité des réseaux est vaste et en pleine évolution. Le champ d'étude englobe un bref historique remontant aux débuts d'Internet et le développement actuel de la sécurité des réseaux. Pour comprendre les recherches menées aujourd'hui, il est nécessaire d'avoir des connaissances de base sur l'internet.

Mots clés : Firewall, Cryptage, Protocole, Adresse IP.

Table des Matières

Liste des Figures

Listes des Acronymes

AH	Authentication Header
ARP	Adress Resolution Protocol
AMS	Anti-Malware systems
DoS	Denial of Service Attack
DDoS	Distribution Denial of Service Attack
DMZ	Demilitarized Zone
ESP	Encapsulation Security Payload
FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
IIS	Internet Information Service
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ICMP	Internet Control Messaging Control
MAC	Media Access Control
MD5	Message Digest5
NAT	Network Adress Translator
PKE	Public Key Exchange
SSL	Secure Socket Layer
SSH	Secure Shell
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

Introduction générale

Introduction générale :

Le monde est de plus en plus interconnecté grâce à l'approche du Web et aux technologies d'organisation non utilisées, ce qui en fait une ville mondiale. Il existe une somme considérable de données individuelles, commerciales, militaires et gouvernementales sur les cadres d'organisation dans le monde. La sécurité de l'organisation devient d'une importance extraordinaire en raison de la propriété intellectuelle qui peut être effectivement acquise par le biais du Web. La sécurité de l'organisation doit donc surveiller les systèmes informatiques organisés et garantir les données électroniques qui sont soit stockées sur les ordinateurs organisés, soit transmises sur les systèmes. L'Internet, qui repose sur les protocoles de communication IP, est devenu la principale innovation en matière d'organisation informatique. Étant donné que l'IP est une innovation d'échange par stockage et transfert, où les informations sont transmises à l'aide de routeurs contrôlés par d'autres personnes, le client A peut consulter les informations du client B qui passent par l'IP du client A.

Dans notre projet nous avons étudié le concept de sécurité des ordinateurs et des réseaux aussi les différentes attaques de sécurité. Nous avons basé dans le deuxième chapitre sur le pare-feu(firewalls) qui fait partie de la sécurité de chaque système informatique et surveille le trafic entrant et/ou sortant et décide s'il doit bloquer un paquet particulier ou le laisser passer ensuite on a parlé sur la nécessité et les différents types de firewalls, à la fin on a expliqué la conception d'une infrastructure sécurisée et ses avantages et inconvénients.

Dans le dernier chapitre nous allons appliquer un filtrage sur un firewall de type fortigate en bloquant certains sites web ainsi que des applications, et par la suite nous allons effectuer des tests d'acceptance.

CHAPITRE I

Concepts de sécurité des ordinateurs et des réseaux

I. 1. Introduction

Lorsque l'on parle de sécurité des organisations, il faut souligner que l'ensemble du dispositif est sécurisé. La sécurité des réseaux ne concerne pas la sécurité des ordinateurs à chaque extrémité de la chaîne de communication. Lors de la transmission d'informations, le canal de communication ne doit pas être à l'abri des attaques. Un programmeur peut viser le canal de communication, obtenir l'information, la déchiffrer et réinsérer un message erroné. La sécurisation de l'arrangement est tout aussi importante que la sécurisation des ordinateurs et le brouillage du message. La sécurité informatique, quant à elle, consiste à prendre des mesures pour sécuriser un seul ordinateur. En sécurisant un seul ordinateur, c'est préoccupé de garantir les actifs stockés sur cet ordinateur et de le protéger des dangers.

I.2. Concepts sous-jacents de la sécurité des ordinateurs et des réseaux :

Les missions de la sécurité organisée sont de fournir le confidentialité, l'intégrité, la non-répudiation, l'authenticité et la disponibilité des informations de valeur qui sont transmises dans des systèmes ouverts ou stockées dans des ordinateurs organisés.

- **Confidentialité :** Éviter la divulgation non autorisée d'informations.
- **Intégrité :** Prévention de l'altération non autorisée des informations.
- **Disponibilité :** Garantir que les systèmes fonctionnent rapidement et que les services ne sont pas refusés aux utilisateurs autorisés.
- **Authenticité :** La propriété d'être honnête et de pouvoir être confirmée et faire confiance. Cela implique de confirmer que les clients sont bien ceux qu'ils prétendent être et que chaque entrée arrivant au cadre provient d'une source fiable.
- **Non-répudiation :** Capacité à garantir que quelqu'un ne peut pas nier ses activités.

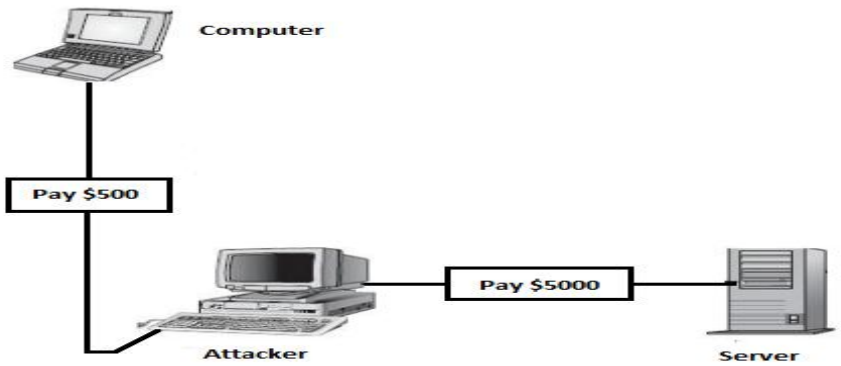
I.2.1. Confidentialité :

La protection des limitations autorisées sur l'accès et la révélation des données, en comptant les implications pour sécuriser la sécurité individuelle et les données exclusives. Les termes "sécurité" et "mystère" sont parfois utilisés pour faire la distinction entre la sécurité des informations individuelles (vie privée) et l'assurance que les informations ont leur place dans une organisation (mystère). Lorsque vous examinez les questions de confidentialité, vous pouvez également vous demander si vous devez simplement dissimuler la substance d'un document à une personne non autorisée, ou sa présence. Vous voudrez considérer la

confidentialité des informations à la fois lorsqu'elles sont rangées sur un ordinateur et lorsqu'elles sont transmises par l'organisation. On peut également penser à garantir la confidentialité des informations stockées sur des tablettes ou des gadgets détachables, tels qu'une clé USB. Il y a eu quelques épisodes ultérieurs, notamment des tablettes perdues qui stockent des informations privées.

I.2.2. Intégrité :

Il est très difficile de donner une brève définition de l'intégrité. En général, l'intégrité consiste à s'assurer sans aucun doute que tout est ce qu'il est censé être et, dans le cadre de la sécurité informatique, à éviter toute modification non autorisée de l'information. L'Orange Book (ou Trusted Computer Framework Assessment Criteria, créé par la Joined States Division of Defense) caractérise l'intégrité de cette manière : c'est l'état dans lequel se trouve une information informatisée qui est identique à celle contenue dans les enregistrements sources et qui n'a pas été exposée à une modification ou à une destruction involontaire ou nocive. L'intégrité est également un problème lorsque l'information est transmise par un réseau. L'intégrité est également un problème lorsque les informations sont transmises par le biais d'un réseau. Un agresseur peut capturer et modifier des paquets d'informations sur le réseau si l'intégrité de ces données n'est pas garantie. Ce type d'attaque est connu sous le nom d'attaque



"man-in-the-middle".

Figure I.1: Une attaque de type "man-in-the-middle" qui modifie le contenu du paquet.

I.2.3. Disponibilité :

Dans le cadre de la sécurité, nous devons garantir qu'un agresseur malveillant ne peut pas empêcher les véritables clients d'avoir un accès raisonnable à leurs cadres. En d'autres termes, nous devons empêcher le refus de service. L'une des principales attaques par déni de service, l'attaque par schtroumpf, est décrite ci-dessous. Une attaque de schtroumpf exige de

l'agresseur qu'il parodie (en s'imaginant être quelqu'un qu'il n'est pas) la personnalité de la victime.

Dans une attaque de schtroumpf, l'agresseur envoie une demande de réverbération ICMP (Internet Control Informing Convention) à l'adresse de diffusion de quelques organisations avec une adresse d'expéditeur usurpée (l'adresse de la victime). La demande réverbérée sera diffusée à tous les hubs de cette organisation. Chaque hub répondra à l'adresse de l'expéditeur usurpée, inondant la victime de paquets de réponses.

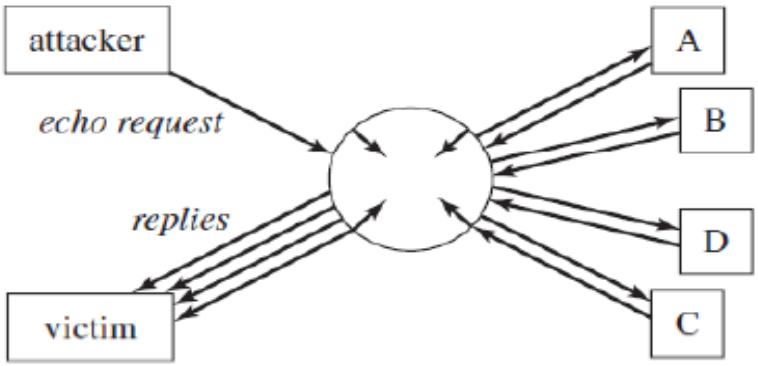


Figure I.2: A denial-of-service attack (smurf attack) [1].

I.2.4. Authenticité :

L'authenticité est la confirmation qu'un message, un échange ou tout autre échange de données provient de la source qu'il prétend être. L'authenticité comprend la confirmation de l'identité, que l'on peut confirmer par l'authentification. En règle générale, la méthode de confirmation comprend plus d'une "vérification" de la personnalité (bien qu'une seule puisse être suffisante). La confirmation peut être quelque chose que l'utilisateur connaît, comme un mot secret. Ou bien, un client peut démontrer sa personnalité avec quelque chose qu'il possède, comme une carte-clé. Les cadres de pointe (biométriques) peuvent en outre fournir une vérification basée sur quelque chose relative à l'utilisateur. Les stratégies de confirmation biométrique comprennent des éléments tels que la marque unique, la géométrie de la main ou la rétine.

I.2.5. Non-répudiation :

Les administrations de non-répudiation typiques dans la sécurité des communications sont la non-répudiation de l'origine, qui fournit la preuve de l'expéditeur d'une archive, et la non-répudiation de la livraison, qui fournit la preuve approximative de la vérité qu'un message a été transmis à un destinataire particulier. Une fois que vous l'avez fait, une personne doit

signer sur la lettre. Cela peut être une illustration de la non-répudiation de la transmission puisque vous démontrerez que la lettre a été remise. Bien sûr, la personne qui signe sur la lettre peut ne pas être celle à qui la lettre a été tendue. Ceci soulève une faille potentielle dans la non-répudiation.

Supposons que la personne qui signe la lettre fabrique le titre du destinataire. Cela implique que la cession peut être refusée (niée) par le véritable destinataire.

I.3. Attaques de sécurité :

Les méthodes courantes d'attaque Internet sont divisées en catégories. Certaines attaques acquièrent des connaissances sur le système ou des renseignements personnels, comme l'écoute clandestine (Eavesdropping) et l'hameçonnage (phishing). Les attaques peuvent également interférer avec la fonction prévue du système, tels que les virus, les vers et les chevaux de Troie.

L'autre forme d'attaque est quand les ressources du système sont consommées inutilement ceux-ci peuvent être causés par l'attaque de déni de service (DoS). D'autres formes d'intrusion sur le réseau existent également, comme les attaques **de schtroumpfs [2].**

I.3.1. Écoute clandestine :

Un « Eavesdropping » est l'interception de communications par une partie non autorisée à l'aide d'un dispositif réseau et d'un renifleur de paquets. Un sniffer de paquet ou un sniffer de réseau est un programme pour surveiller le trafic de réseau entrant. « TCPdump » et « Wireshark » (anciennement connus « Ethereal ») sont les deux renifleurs réseau les plus utilisés. L'écoute passive est quand la personne n'écoute que secrètement les messages en réseau. D'autre part, l'espionnage actif est quand l'intrus écoute et insère quelque chose dans le flux de communication. [**2]**

I.3.2. Déni de service :

Les attaques par « Denial of Service » empêchent les utilisateurs légitimes d'obtenir des services qu'ils peuvent normalement obtenir des serveurs. De telles attaques forcent souvent l'ordinateur cible à traiter un grand nombre de choses inutiles, espérant consommer toutes ses ressources critiques. Une attaque par « Denial of Service », dénotée par le DoS, peut être lancée à partir d'un seul ordinateur, ou à partir d'un groupe d'ordinateurs distribués sur Internet. Cette dernière attaque est signalée par DDoS. L'attaque schtroumpf est un type typique d'attaque

DoS, où l'attaquant envoie des requêtes ping contrefaites à un grand nombre d'ordinateurs dans un court laps
de temps, où l'adresse IP source dans la requête ping contrefaite est remplacée par l'adresse IP de la victime.

I.3.3. Usurpation d'identité :

Les attaques par « Identity spoofing » permettent aux agresseurs d'usurper l'identité d'une victime sans utiliser les mots de passe de la victime. Les attaques usuelles d'identité courantes comprennent les attaques de l'homme au milieu, les rediffusions de messages, l'usurpation de réseau et les attaques d'exploitation de logiciels.

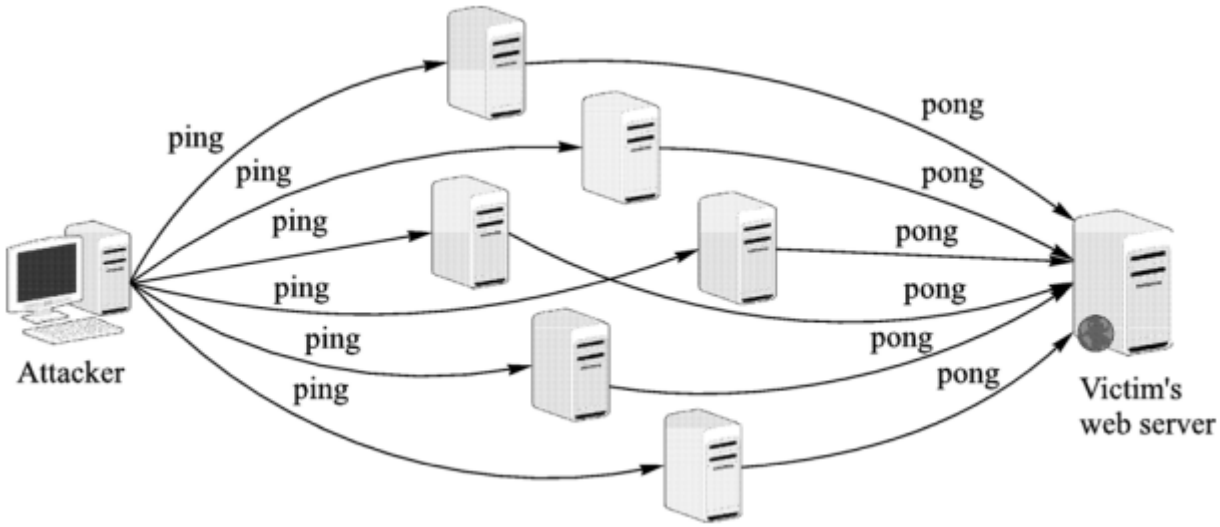


Figure I.3: Distributed denial of service [3].

I.3.3.1. Attaques de type « Man-in-the-middle » (intermédiaire) :

Dans une attaque « Man-in-the-middle », l'attaquant tente de compromettre un périphérique réseau (ou installe l'un des siens) entre deux ou plusieurs utilisateurs. À l'aide de ce dispositif, l'attaquant peut intercepter, modifier ou fabriquer des données transmises entre les utilisateurs. L'attaquant transmettra alors les paquets modifiés (données) comme s'ils n'avaient pas été touchés par l'attaquant. Par exemple, l'attaquant peut intercepter un paquet IP envoyé par l'utilisateur 1, modifier sa charge utile, puis envoyer le paquet modifié à l'utilisateur 2 comme s'il venait de l'utilisateur 1

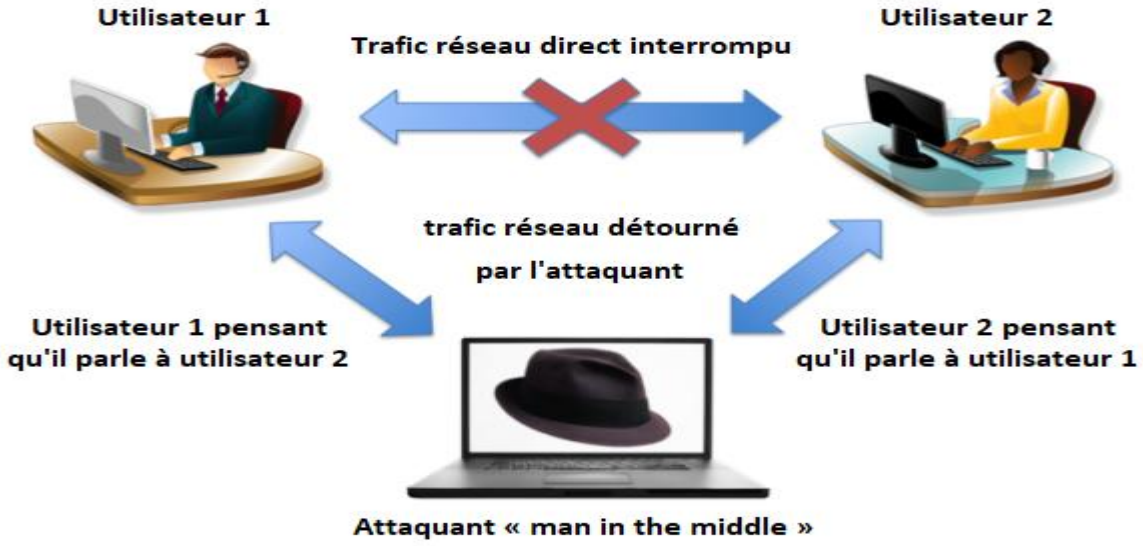


Figure I.4: Attaque de type « Man-in-the-middle ».

I.3.3.2. Mystification du réseau :

Le « IP-Spoofing » est l'une des principales techniques d'usurpation de réseau. Il se compose de l'inondation SYN, Le détournement TCP, et L'usurpation d'ARP. L'usurpation d'ARP est également appelée empoisonnement ARP.

- **L'inondation SYN « SYN Flooding » :**

L'inondation SYN exploite un effet secondaire d'implémentation des protocoles réseau TCP/IP. Dans une attaque d'inondation SYN, l'attaquant remplit le tampon TCP de l'ordinateur cible avec un grand volume de paquets de contrôle SYN, rendant l'ordinateur cible incapable d'établir des communications avec d'autres ordinateurs. Lorsque cela se produit, l'ordinateur cible est appelé *un ordinateur muet ou un* ordinateur silencieux.

Pour lancer une attaque d'inondation SYN contre un ordinateur cible, l'attaquant lui envoie un grand nombre de paquets SYN contrefaits, chacun demandant d'établir des connexions TCP. Le terme *paquet SYN conçu* signifie que l'adresse source contenue dans le paquet SYN est une adresse IP légitime, mais l'ordinateur hôte sur cette adresse n'est pas accessible. Cet ordinateur hôte peut être mis hors tension ou hors réseau. L'attaquant utilise des paquets SYNpacket pour éviter d'être traqué. Et il utilise une adresse IP source légitime pour s'assurer que les paquets SYNpacket seront livrés à leur destination, parce que le serveur de noms de domaine va supprimer les paquets IP avec de fausses adresses IP. Selon la procédure de poignée de main à trois dans le protocole TCP, l'ordinateur de la victime est obligé d'envoyer un paquet ACK à l'adresse IP source contenue dans le paquet SYN qu'il reçoit, et attend qu'un

paquet ACK soit renvoyé à partir de cette adresse IP. Cependant, l'ordinateur hôte avec cette adresse IP source n'est pas accessible et ne répond donc pas. Ainsi, l'ordinateur de la victime ne recevra jamais le paquet ACK qu'elle attend, forçant le paquet SYNpacket à rester dans le tampon TCP jusqu'à ce que sa durée de vie expire. Pendant cette période, le tampon TCP est complètement occupé par (c.-à-d. inondé de) paquets SYN fabriqués, et donc l'ordinateur de la victime n'aura pas de place dans le tampon TCP pour établir une nouvelle connexion avec un autre ordinateur. L'ordinateur de la victime est alors considéré comme muet [3]**.**

- **Le détournement TCP « TCP Hijacking » :**

Au cours d'une session TCP/IP (Transmission Control Protocol/Internet Protocol) normale entre un serveur et un client, le client lance un contact à trois avec le serveur en envoyant un message SYN. Un message SYN est utilisé pour demander la synchronisation d'un numéro de séquence.

Supposons que l'ordinateur V est un ordinateur de l'entreprise et que l'utilisateur A est un employé de cette entreprise et qu'il se connecte à l'ordinateur V à partir de chez lui. L'ordinateur de l'utilisateur A envoie un paquet de contrôle SYN à V et suppose maintenant qu'un attaquant intercepte ce paquet. L'attaquant utilise alors l'attaque d'inondation SYN pour désactiver l'ordinateur V, de sorte que V ne peut pas terminer le protocole de poignée de main à trois voies avec l'ordinateur de l'utilisateur A. Si l'attaquant peut prédire le bon numéro de séquence TCP pour le paquet ACK qui est censé être envoyé à A à partir de l'ordinateur en sourdine V, alors l'attaquant peut créer un paquet ACK et l'envoyer à l'ordinateur de l'utilisateur A. Le paquet ACK conçu utilise le bon numéro de séquence TCP et l'adresse IP de V comme adresse IP source.

L'ordinateur de l'utilisateur A reçoit le paquet ACK et vérifie qu'il a le bon numéro de séquence TCP. Il envoie ensuite un paquet ACK à l'attaquant pour compléter la procédure de poignée de main à trois voies avec l'attaquant. Ainsi, la connexion TCP que l'ordinateur de l'utilisateur A a établie est avec l'attaquant, au lieu de V. Puisque l'en-tête du protocole TCP ne contient pas l'adresse IP source, le logiciel de la couche TCP ne vérifierait pas la légitimité des adresses IP contenues dans l'en-tête IP. Le protocole IP achemine le paquet IP qu'il reçoit vers la destination en fonction des informations contenues dans l'en-tête IP. Il ne garde pas trace des informations d'en-tête des paquets IP précédents qu'il a reçus. Ainsi, vérifier l'adresse IP source à la couche IP n'aide pas à identifier si l'adresse IP source dans le paquet IP courant est la même que celles des paquets IP précédents. Cela montre que le fonctionnement de la suite de protocoles TCP/IP (sa première implémentation en particulier) rend possible le

détournement de TCP. Pour arrêter le détournement TCP, il est important d'utiliser un logiciel (p. ex., des enveloppeurs TCP) qui vérifie les adresses IP de la couche TCP. **[3]**

- **L'usurpation d'ARP « ARP Spoofing » :**

Les ordinateurs sont identifiés par des adresses MAC (media access control) uniques. Les adresses MAC sont également appelées adresses physiques. ARP est un protocole de résolution d'adresse à la couche lien, qui convertit l'adresse IP de destination dans l'en-tête IP à l'adresse MAC de l'ordinateur sous-jacent au réseau de destination. Dans une attaque de spoofing ARP, l'attaquant change l'adresse MAC légitime d'une adresse IP à une adresse MAC différente choisie par l'attaquant.

Pour éviter les attaques d'usurpation ARP, la vérification est la clé. En particulier, nous devrions renforcer les procédures de vérification des adresses MAC et des noms de domaine, et nous assurer que l'adresse IP source et l'adresse de destination dans un paquet IP n'ont pas été changées pendant les transmissions.

I.3.3.3. Attaques par rejeu :

Dans une attaque « message replay », l'attaquant intercepte d'abord un message légitime, le garde intact, puis le retransmet plus tard au récepteur original. Dans certains protocoles d'authentification, par exemple, après que l'utilisateur « A » s'est révélé au système en tant qu'utilisateur légitime, il recevra une passe d'authentification. Avec ce laissez-passer, elle pourra obtenir des services fournis par le système. Cette passe est cryptée et ne peut donc pas être modifiée. Cependant, l'attaquant peut l'intercepter, en garder une copie et l'utiliser plus tard pour usurper l'identité de l'utilisateur A afin d'obtenir les services du système.

Les mécanismes courants pour contrecarrer les attaques par rejeu de message :

- Apposez un horodatage sur le message. Lorsqu'un utilisateur reçoit un message dont l'horodatage est ancien, il sait que ce message est une relecture. Cette méthode, cependant, exige que tous les ordinateurs en réseau soient synchronisés avec peu d'erreur. Bien qu'il ne s'agisse pas d'un problème dans les réseaux locaux, il est difficile d'obtenir une synchronisation précise dans les réseaux étendus.
- La meilleure méthode pour contrecarrer les attaques de relecture de message est d'utiliser un nonce et un temps. Estampiller ensemble. En utilisant cette méthode, la synchronisation n'a pas besoin d'être très précise et l'utilisateur n'a besoin que de suivre le nonce qu'il rencontre dans un intervalle de temps court et fixe. L'utilisateur stocke un nonce dans un enregistrement avec un horodatage lorsqu'il est enregistré pour la première fois. Lorsque ce timbre devient vieux, le nonce est retiré. Un message n'est considéré comme une relecture

que lorsque son non est déjà dans l'enregistrement ou que son horodatage est en dehors de l'intervalle de temps [3]**.**

I.3.4. Intrusion :

L'intrusion dans la sécurité du réseau signifie qu'un utilisateur illégitime, c.-à-d. l'intrus, accède aux systèmes informatiques de quelqu'un d'autre. L'intrus peut transformer l'ordinateur de la victime en son propre serveur, ce qui peut entraîner le vol de ressources informatiques et de bande passante réseau de la victime. L'intrus peut également voler des informations utiles se trouvant dans l'ordinateur de la victime. Les failles de configuration, les défauts de protocole et les effets secondaires des logiciels peuvent tous être exploités par des intrus. L'ouverture des ports TCP ou UDP qui ne doivent pas être ouverts est une faille de configuration courante. Les ports TCP et UDP sont des points d'entrée des programmes d'applications réseau.

La détection des intrusions est une technologie de détection des intrusions. Fermer les ports TCP et UDP qui peuvent être exploités par des intrus peut également aider à réduire les intrusions.

Les « IP scans » et « port scans » :

Les scans IP et les scans de ports sont des outils de piratage courants. IP scanne la recherche d'adresses IP existantes sur Internet, et le port scanne la recherche de ports ouverts sur un ordinateur. Les attaquants utilisent des scans IP pour rechercher des cibles potentielles et utilisent des scans de ports pour identifier les ports ouverts qui sont vulnérables dans les cibles. Cependant, les scans de ports peuvent également aider les utilisateurs à identifier dans leurs propres systèmes quels ports sont ouverts et quels ports peuvent être vulnérables.

I.3.5. Softwares malveillants :

Les logiciels destinés à nuire aux ordinateurs sont des logiciels malveillants. Les logiciels malveillants. Les formes courantes de logiciels malveillants comprennent les virus, les vers, les chevaux de Troie et les logiciels espions.

I.3.5.1. Virus et « Worms » :

Un virus informatique est un logiciel qui peut se reproduire. Un programme ou un fichier qui contient un virus est appelé un hôte infecté. Un hôte non infecté est aussi appelé un hôte sain. Lorsqu'un hôte infecté est transmis à un autre ordinateur, le virus qui y vit est également transmis. L'exécution d'un virus est initiée par l'hôte infecté. À savoir, seulement quand un

programme infecté est exécuté ou un fichier infecté est ouvert, un virus contenu dans lui peut être exécuté. Lorsqu'il est exécuté, un virus peut nuire (p. ex., supprimer des fichiers système) au système où réside son hôte ou se répliquer pour infecter d'autres hôtes sains du système. Un ver d'ordinateur est également un morceau de logiciel qui peut se reproduire. Un ver peut s'exécuter à tout moment. Lorsqu'il est exécuté, un ver peut nuire au système où il réside ou se répliquer à d'autres systèmes par l'intermédiaire de réseaux.

Il existe deux mesures communes pour combattre les virus et les vers. Une mesure déploie des analyses de virus pour détecter, mettre en quarantaine et supprimer les hôtes et les vers infectés. L'autre mesure, composée des règles suivantes, empêche les virus et les vers d'entrer dans un ordinateur :

- ✓ Ne téléchargez pas de software (par exemple jeux) à partir de sites Web non approuvés ou d'autres sources.
- ✓ N'ouvrez aucun fichier exécutable qui vous a été donné par quelqu'un que vous ne connaissez pas.
- ✓ S'assurer que les correctifs logiciels sont installés et à jour.

I.3.5.2. Chevaux de Troie :

Dans le domaine de la sécurité des réseaux, les chevaux de Troie sont des logiciels qui semblent faire une chose, mais qui exécutent secrètement d'autres tâches. Les chevaux de Troie se déguisent souvent en applications logicielles souhaitables et inoffensives pour attirer les gens à les télécharger. Lorsqu'elles sont exécutées par l'utilisateur, les fonctions cachées qu'elles contiennent et qui ont désormais les droits d'accès de l'utilisateur font secrètement du mal. Jeux et outils de gestion de réseau disponibles pour des téléchargements gratuits à partir de sites Web inconnus sont souvent des chevaux de Troie. Les chevaux de Troie peuvent également utiliser des noms attrayants tels que AntiSpyWare.exe ou Real_Player.exe (notez que le vrai est RealPlayer.exe) pour piéger les utilisateurs à les utiliser. Les mêmes mesures de lutte contre les virus et les vers peuvent également être utilisées pour combattre les chevaux de Troie. Les analyses de virus peuvent également détecter, mettre en quarantaine et supprimer les chevaux de Troie.

CHAPITRE II

Firewalls et Mécanismes de sécurité

II.1. Introduction :

Une infrastructure réseau est vulnérable aux attaques à de nombreux niveaux. Par exemple, nous devons nous préoccuper des données qui résident sur les périphériques physiques et qui transitent par les commutateurs et les routeurs du réseau. Nous devons également réfléchir à la manière de sécuriser physiquement les périphériques réseau, car quelle que soit la force de notre sécurité, elle peut être interrompue par une personne ayant un accès physique aux périphériques réseau.

Sécuriser physiquement nos propres appareils est une chose, mais sur un réseau public comme Internet, on ne contrôle pas les appareils sur lesquels nos données pourraient passer. On doit concevoir une stratégie de sécurité qui réduit les risques associés au déplacement des données sur les réseaux.
Pour la plupart des entreprises, des institutions gouvernementales et des organismes financiers, il est nécessaire de protéger leurs réseaux privés et leurs établissements de communication.

Cependant, de nombreuses associations ont des exigences commerciales qui les obligent à connecter leur réseau privé à Web ou à d'autres réseaux à grande échelle qui sont standard natures non sécurisés. Chaque fois qu'on se connecte à un réseau non sécurisé, tel qu'Internet, on ouvre une expansive porte aux attaques potentielles. L'une des meilleures façons de se prémunir contre les attaques provenant du réseau non sécurisé est d'utiliser des firewalls au point d'association du réseau non sécurisé et du réseau interne.

II.2. Définition d'un Firewall :

Un Firewall peut être un dispositif matériel, un logiciel ou une combinaison des deux. Il est utilisé comme une barrière entre l'Internet et un réseau périphérique. Les Firewalls examinent les paquets participants et sortants et déterminent s'ils doivent les laisser passer ou les bloquer. Un paquet qui est bloqué sera retiré du réseau.

Les paquets qui entrent dans le réseau interne depuis l'extérieur doivent être évalués avant d'être autorisés à y pénétrer. L'un des éléments critiques d'un firewall est sa capacité à examiner les paquets sans imposer un affect négatif sur la vitesse de communication tout en fournissant des protections de sécurité pour le réseau interne.

Aujourd'hui, les firewalls sont intégrés dans des périphériques réseaux courants, notamment les routeurs, les commutateurs, les modems et les points d'accès sans fil. Les

firewalls matériels sont rapides, mais ils sont difficiles à mettre à jour. Les firewalls logiciels, quant à eux, sont plus lents, mais plus faciles à mettre à jour.

L'inspection des paquets effectuée standard les firewalls peuvent être réalisés à l'aide de plusieurs méthodes différentes. Selon la méthode particulière utilisée standard le firewall, il peut être caractérisé comme un filtre de paquets, une passerelle de circuit, une passerelle d'application ou un filtre de paquets dynamique.

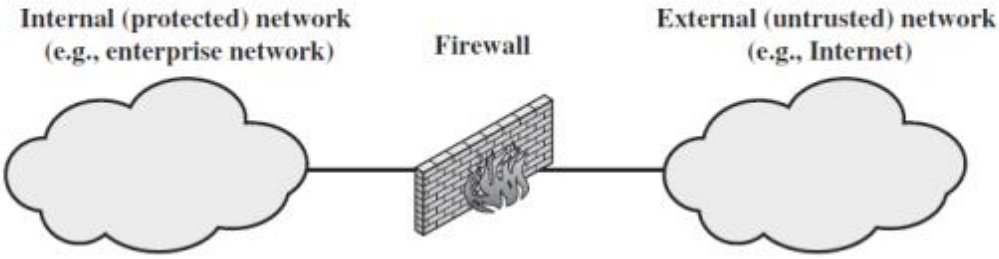


Figure II.1: Un exemple de firewall entre deux réseaux [2].

II.3. Nécessité et Caractéristiques des Firewall :

La connectivité Web n'est plus facultative pour les associations. Les informations et les administrations disponibles sont essentielles pour l'organisation. De plus, les utilisateurs individuels au sein de l'organisation veulent et ont besoin d'un accès à Web, et si celui-ci n'est pas fourni standard leur réseau local, ils utiliseront la fonction d'accès commuté de leur PC à un fournisseur de administrations Web (ISP). Cependant, si l'accès à Web apporte des avantages à l'organisation, il permet au monde extérieur d'atteindre et d'interagir avec les ressources du réseau local. Cela constitue un danger pour l'organisation. S'il est possible d'équiper chaque poste de travail et chaque serveur du réseau de l'entreprise de solides dispositifs de sécurité, tels qu'une assurance contre les interruptions, cela peut ne pas être suffisant et, dans certains cas, ne pas être rentable. Prenons l'exemple d'un réseau composé de centaines, voire de milliers de systèmes fonctionnant sous différents systèmes d'exploitation, tels que différentes adaptations d'UNIX et de Windows. Lorsqu'une faille de sécurité est découverte, chaque système potentiellement affecté doit être mis à niveau pour corriger cette faille. Cela nécessite une gestion de l'arrangement évolutif et des correctifs agressifs pour fonctionner efficacement.

Bien que difficile, cela est possible et nécessaire si seule la sécurité basée sur l'hôte est utilisée. Une alternative largement acceptée, ou du moins un complément aux administrations de sécurité basée sur l'hôte, est le firewall.

Tout le trafic de l'intérieur vers l'extérieur et vice versa doit passer standard le firewall, ce qui est réalisé en bloquant physiquement tout accès au réseau local sauf via le firewall. Seul le trafic autorisé, tel que défini standard la politique de sécurité locale, sera autorisé à passer. Différents sorts de firewall sont utilisés, qui mettent en œuvre différents sorts de politiques de sécurité. Le firewall lui-même est immunisé contre la pénétration. Cela implique l'utilisation d'un système durci avec un système d'exploitation sécurisé. Les systèmes informatiques de confiance conviennent pour héberger un firewall et sont souvent requis dans les applications gouvernementales.

II.4. Politiques de sécurité du firewall :

Pour protéger les réseaux privés et les machines individuelles des dangers du grand Web, un firewall peut être utilisé pour filtrer le trafic participant ou sortant en fonction d'un ensemble prédéfini de règles appelées politiques de firewall.

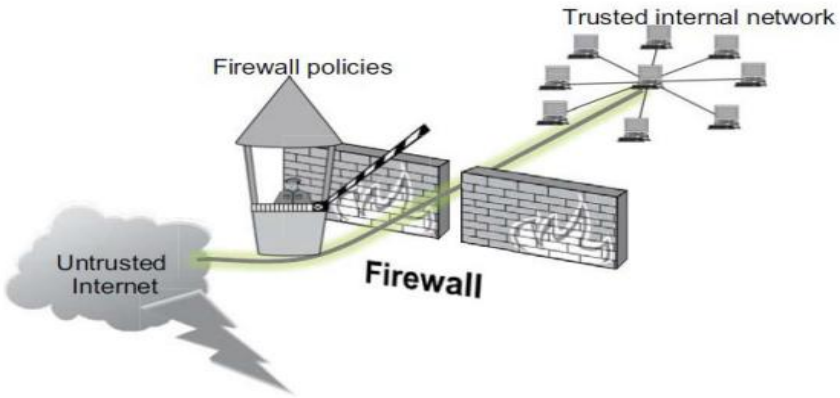


Figure II.2: Trafic passant par un firewall en fonction des politiques [6].

II.4.1. Actions de politique :

Les paquets traversant un firewall peuvent avoir l'un des trois résultats suivants :

Acceptés : autorisés à traverser le firewall.

Abandonné : non autorisé à passer, sans indications d'échec.

Rejeté : non autorisé à passer, accompagné d'une tentative d'informer la source que le paquet a été rejeté.

II.5. Techniques de control d'accès utilisées par les firewalls :

- **Contrôle des services** : Détermine les sorts d'administrations Web auxquels il est possible d'accéder, en entrée ou en sortie. Le firewall peut filtrer le trafic sur la base de l'adresse IP, du protocole ou du numéro de port ; il peut fournir un logiciel proxy qui reçoit et interprète

chaque demande de service avant de la transmettre ou il peut héberger le logiciel serveur lui-même, tel qu'un service Web ou de messagerie.

- **Contrôle de direction** : Détermine la direction dans laquelle des demandes de service particulières peuvent être initiées et autorisées à traverser le firewall.
- **Contrôle de l'utilisateur** : Contrôle l'accès à un service en fonction de l'utilisateur qui tente d'y accéder. Cette fonction est généralement appliquée aux utilisateurs à l'intérieur du périmètre du firewall (utilisateurs locaux). Elle peut également s'appliquer au trafic participant provenant d'utilisateurs externes, ce qui nécessite une certaine forme de technologie d'authentification sécurisée, telle que celle fournie standard IPsec.
- **Contrôle du comportement** : Contrôle la façon dont certaines administrations sont utilisées. Standard exemple, le firewall peut filtrer le courrier électronique pour éliminer les pourriels, ou il peut permettre l'accès externe à une partie seulement des informations d'un serveur Web local.

II.5.1 Limites des firewalls :

A. -Le firewall ne peut pas protéger contre les attaques qui le contournent. Les systèmes internes peuvent être dotés d'une fonction d'accès commuté pour se connecter à un fournisseur d'accès Web. Un réseau local interne peut prendre en charge un pool de modems qui fournit une capacité d'association aux employés en déplacement et aux télétravailleurs.

B. -Le firewall peut ne pas protéger complètement contre les menaces internes, comme un employé mécontent ou un employé qui coopère volontairement avec un attaquant externe.

C. -Un réseau local sans fil mal sécurisé peut être open de l'extérieur de l'organisation. Un firewall interne qui sépare des parties d'un réseau d'entreprise ne peut pas se prémunir contre les communications sans fil entre des systèmes locaux situés de différents côtés du firewall interne.

D. -Un ordinateur versatile, un PDA ou un dispositif de stockage portable peut être utilisé et infecté en dehors du réseau d'entreprise, puis attaché et utilisé en interne.

II.6. Types des firewalls:

II.6.1. Les firewalls bridge:

Ils ont généralement une grande portée. Ils agissent comme de véritables câbles d'organisation avec le travail inclus de tamisage, d'où leur titre de bridge. Leurs interfaces n'ont pas d'adresse IP et échangent en quelque sorte des paquets d'une interface à l'autre en appliquant des règles prédéfinies. Cette non-attention est particulièrement précieuse, car elle implique que le firewall

est imperceptible pour un programmeur typique. Sans aucun doute, lorsqu'une requête ARP est envoyée sur le câble d'organisation, le firewall ne réagira jamais. Ses adresses Mac ne circuleront jamais sur l'organisation, et puisqu'il ne fait que "forwarder" des paquets, il sera totalement indétectable sur l'organisation. Il est donc incompréhensible d'attaquer le firewall directement, car aucun paquet ne sera traité par le firewall comme son propre objectif. La seule façon de le contourner est donc de passer outre ses règles d'exclusion. Toute attaque devra "négocier" avec ses règles et tenter de les contourner [8].

Dans la plupart des cas, ils disposent d'une interface d'arrangement cloisonnée. Un câble s'interface avec une troisième interface, série ou Ethernet, qui doit être utilisée de temps en temps, idéalement dans un environnement sécurisé. Ces firewalls se trouvent généralement sur les commutateurs (switches).

II.6.1.1. Avantages :

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

II.6.1.2. Inconvénients :

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

II.6.2. Les firewalls matériels :

On les trouve souvent sur les routeurs achetés sur le marché par de grands fabricants comme Cisco ou Huawei ! Intégrés directement dans la machine, ils agissent comme une "boîte noire" et s'intègrent parfaitement au matériel. Leur configuration est souvent relativement ardue, mais leur avantage est que leur interaction avec les autres fonctionnalités du routeur est simplifiée par leur présence sur le même équipement réseau. Souvent relativement peu flexibles en termes de configuration, ils sont également peu vulnérables aux attaques, car ils sont présents dans la "boîte noire" qu'est le routeur. De plus, comme ils sont souvent étroitement liés au matériel, l'accès à leur code est assez difficile, et le fabricant a eu la liberté de produire des systèmes de code "signé" pour authentifier le logiciel (système RSA ou similaire). Ce système n'est implémenté que dans les firewalls haut de gamme, car il évite de remplacer le logiciel par un autre non produit par le fabricant, ou de le modifier, ce qui rend le firewall très sûr. On les trouve régulièrement sur les commutateurs achetés dans la vitrine par d'énormes producteurs

comme Cisco ou Huawei ! Coordonnées spécifiquement dans la machine, elles agissent comme une "boîte noire", et ont une intégration parfaite avec l'équipement. Leur installation est souvent assez difficile, mais leur avantage est que leur interaction avec les autres fonctionnalités du commutateur est modifiée par leur proximité sur le même équipement. Régulièrement modérément difficiles à installer, ils ne sont pas non plus exceptionnellement sans défense contre les attaques, car ils sont visibles dans la "boîte noire" qu'est le commutateur. En outre, comme ils sont souvent étroitement liés à l'équipement, l'accès à leur code est très difficile, et le producteur a eu l'occasion de livrer des cadres de code "marqués" pour confirmer le programme (cadre RSA ou comparable). Ce Framework est en quelque sorte actualisé dans les firewalls haut de gamme, puisqu'il maintient une distance stratégique pour ne pas supplanter le programme informatique par un autre non livré par le producteur, ou l'ajuster, rendant ainsi le firewall exceptionnellement sûr. Son organisation est régulièrement moins exigeante que celle des firewalls à pont, les grandes marques de commutateurs l'utilisant comme un point d'offre. Leur niveau de sécurité est en outre exceptionnellement élevé, sauf pour la découverte de défauts concevables comme plusieurs firewalls. Tout bien considéré, vous devez savoir que vous dépendez entièrement du fabricant de l'équipement pour cette mise à niveau, qui peut être, dans certains cas, très prohibitive. Enfin, pour ainsi dire, les points forts particuliers donnés par le fabricant de l'équipement sont exécutés. Cette dépendance implique que dans le cas où un point fort nous interface sur un firewall d'une autre marque, il est inconcevable de l'utiliser. Il est donc fondamental de décider de ses besoins en cours de route et de sélectionner soigneusement le fabricant de commutateurs (switches) [8].

II.6.2.1. Avantages :

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

II.6.2.2. Inconvénients :

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

II.6.3. Les firewalls logiciels :

Ils sont fréquemment commerciaux et visent à sécuriser un ordinateur spécifique, et non un ensemble d'ordinateurs. Régulièrement payants, ils peuvent être prohibitifs et, dans certains cas,

pas exceptionnellement sûrs. Sans aucun doute, ils sont plus orientés vers la facilité d'utilisation que vers l'exhaustivité, afin de rester disponibles pour le client final [8].

II.6.3.1. Avantages :

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

II.6.3.2. Inconvénients :

- Facilement contournable.
- Difficiles à départager de par leur nombre énorme.

II.7. Considérations relatives à la conception d'une infrastructure sécurisée :

Nous devrons déterminer les vulnérabilités qui affecteront le réseau d'une entreprise, puis tenir compte de l'importance des données ainsi que des coûts et des exigences techniques pour les sécuriser.

- **Déterminer les besoins de sécurisation du trafic réseau :** La sécurisation du trafic réseau nécessite l'utilisation du processeur et de la bande passante réseau. On doit donc déterminer le trafic qui nécessite une sécurité et le niveau de sécurité qu'il nécessite. Cela peut aller de la mise en place d'une connexion point à point à partir du PC qui envoie des données confidentielles au serveur, à l'établissement d'une connexion ou d'un tunnel sécurisé entre les routeurs afin que tout le trafic qui passe par les routeurs sur le segment soit chiffré.
- **Identifiez les problèmes de compatibilité des systèmes d'exploitation :** La version du système d'exploitation ou de l'application que nous exécute affecte les options de sécurité disponibles pour la transmission de données. On doit peser le coût de la mise à niveau du système d'exploitation ou de l'application avec le coût d'être moins sûr.
- **Assurez-vous que le matériel est sécurisé :** Si le matériel n'est pas sécurisé, peu importe les mesures de sécurité qu'on prenne sur les paquets qui traversent notre réseau. La fixation du matériel signifie qu'on doit verrouiller les armoires de câblage et contrôler l'accès à la salle des serveurs. On peut également renforcer la sécurité en utilisant des commutateurs plutôt que des concentrateurs sur le réseau. Un commutateur contrôle le trafic sortant afin qu'il soit dirigé vers le périphérique ou le segment attaché à un port spécifique au lieu d'envoyer tous les paquets à tous les périphériques, ce qui rend plus difficile pour les attaquants de détecter les paquets sur votre réseau.

- **Déterminer les méthodes à utiliser pour sécuriser les données qui seront transmises sur un réseau :** Les données sont vulnérables lors de leur déplacement sur les périphériques physiques et les supports du réseau. On ne peut pas faire confiance à des appareils sur lesquels nous n'exercerons pas un contrôle total, on doit donc prendre les précautions appropriées avec nos données confidentielles. Principalement, on doit déterminer l'identité de la personne et/ou de l'ordinateur qui transmet les données et chiffrer les données afin qu'elles ne puissent pas être lues sur un réseau non sécurisé.

Une fois que nous déterminons les types d'attaques auxquelles nos données sont vulnérables, on doit élaborer un plan pour transmettre les données en toute sécurité sur le réseau. Cela peut impliquer de trouver une méthode pour chiffrer les données que vous transmettez, de vérifier que les données n'ont pas été manipulées en transit et de choisir la méthode que nous utilisera pour authentifier les clients distants sur le réseau.

II.8. Méthodes de sécurisation d'un réseau :

II.8.1. Définition des périmètres de réseau :

Une façon de sécuriser un réseau consiste à isoler les segments qui ont des exigences de transmission de données sécurisées. On peut segmenter un réseau au niveau de la couche 3 à l'aide de routeurs et de sous-réseaux et au niveau de la couche 2 à l'aide de commutateurs et de VLAN.

II.8.1.1. Isolement des réseaux non sécurisés à l'aide de sous-réseaux :

La plupart des organisations ont un périmètre réseau, c'est-à-dire tout point qui connecte le réseau interne à des réseaux externes. Les périmètres réseau comprennent le point de connexion réseau à Internet, les liens vers un bureau satellite ou un serveur d'accès à distance. Un sous-réseau filtré se trouve également sur le périmètre d'un réseau. Un sous-réseau filtré est utilisé comme zone protégée sur le réseau pour exécuter des services partagés en dehors de l'organisation. Parmi les autres utilisations d'un sous-réseau filtré, citons l'isolation de données sécurisées sur un segment ou la mise à l'écart d'un segment dans lequel une activité non sécurisée est courante, comme un environnement de développement logiciel ou un réseau de test.

Une zone démilitarisée (DMZ) est un type de sous-réseau filtré. Il s'agit d'un segment de réseau isolé au point où un réseau d'entreprise rencontre Internet. Les points d'accès sans fil ou les connexions de réseau privé virtuel (VPN) sont d'autres exemples de périmètres de réseau. Le périmètre du réseau est la partie de tout réseau la plus vulnérable aux attaques. L'attaque peut être aléatoire ou ciblée. En raison de la prévalence des menaces qui affectent les points d'accès

au réseau public, vous devez prendre grand soin de minimiser l'exposition de votre réseau interne au réseau public, également appelé l'état sauvage.

Les routeurs et les firewalls peuvent être utilisés pour filtrer le trafic qui passe dans et hors du sous-réseau filtré. Il existe généralement trois types de configurations qu'une organisation peut implémenter lors de la sécurisation de ses périmètres réseau : hôte bastion, configuration à trois volets ou configuration back-to-back (dos à dos).

Hôte Bastion : Un hôte bastion agit comme la seule connexion que les ordinateurs du réseau interne peuvent utiliser pour accéder à Internet (ou à d'autres réseaux externes). Cette configuration est illustrée ci-dessous. Lorsqu'il est configuré comme firewall, l'hôte bastion est spécialement conçu pour prévenir les attaques contre le réseau interne. L'hôte bastion utilise au moins deux cartes réseau : l'un est connecté au réseau interne tandis que l'autre est connecté au réseau externe. Cette configuration sépare physiquement le réseau interne de l'extérieur. Un exemple d'hôte bastion est un ordinateur qui partage une connexion Internet et fournit des services NAT (Network Address Translation), tels qu'un serveur proxy. Sa faiblesse est qu'il s'agit d'un point unique de défaillance, si elle est compromise, l'attaquant peut accéder au réseau interne.

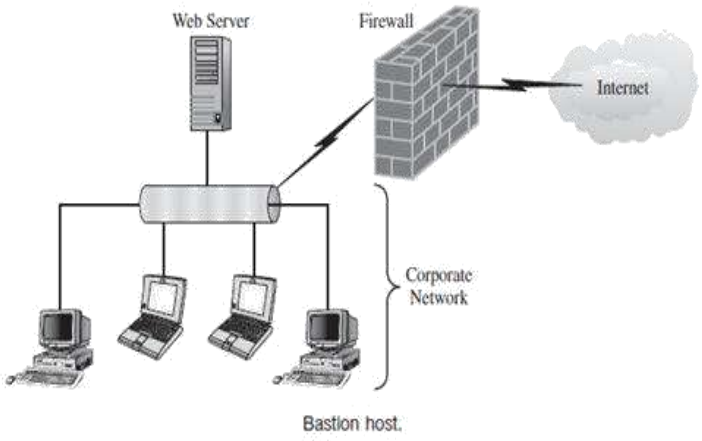


Figure II.3 : Illustration d'un hôte bastion [1]

- **Configuration à trois volets :**

Dans une configuration à trois branches, le système de firewall dispose d'au moins trois cartes réseau. Une carte sera connectée au réseau interne, une au réseau externe ou public et la troisième à un sous-réseau filtré. Cette configuration permet aux hôtes des réseaux publics et internes d'accéder aux ressources disponibles dans le sous-réseau filtré pendant continuer à isoler le réseau interne de la nature. Par exemple, vous pouvez placer un serveur Web dans un sous-réseau filtré. La figure II.2 illustre cette configuration.

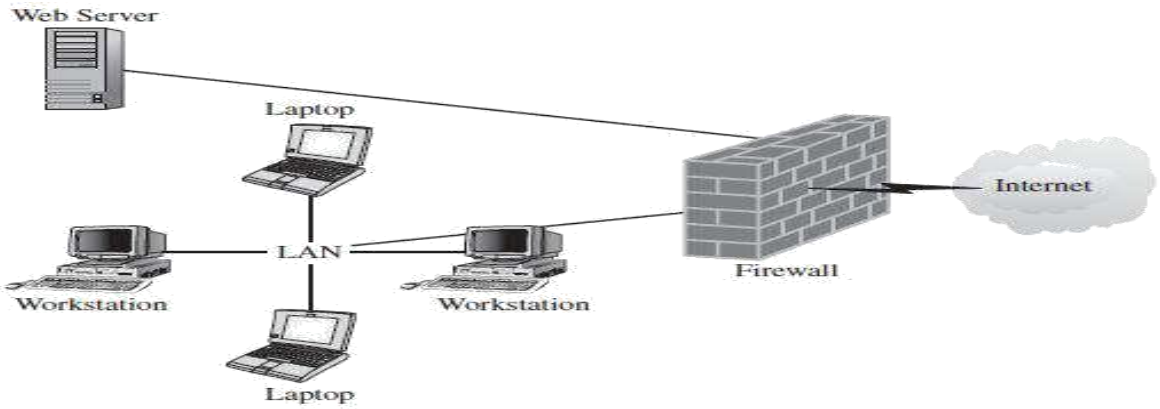


Figure II.4 : configuration à trois branches [1]

- **Configuration back-to-back :**

La configuration back-to-back place le sous-réseau filtré entre deux firewalls. Le sous-réseau filtré est connecté par un firewall à Internet à une extrémité (semblable à un hôte bastion) et est connecté par un autre firewall au réseau interne à l'extrémité opposée. Il s'agit probablement de la configuration la plus sécurisée tout en permettant l'accès aux ressources publiques. Cela nécessiterait qu'un attaquant brise les deux firewalls afin de compromettre le réseau interne. La figure II.3 illustre cette configuration.

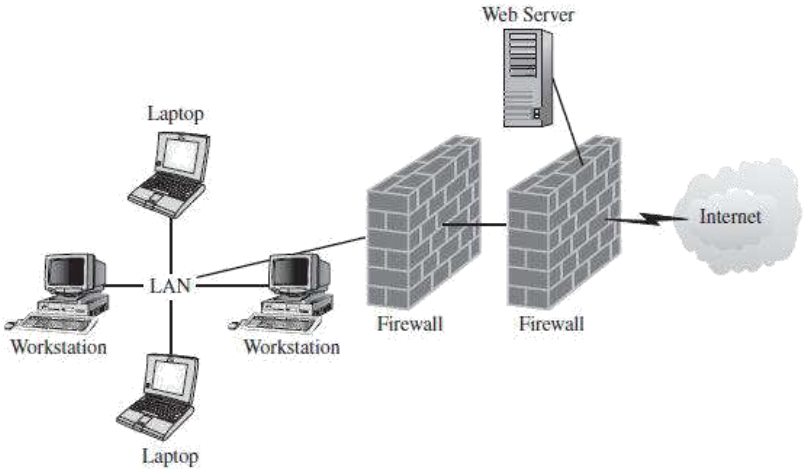


Figure II.5: Configuration «back-to-back» [1].

II.8.1.2. Utilisation de commutateurs (switches) et de VLAN :

Lorsque on segmente un réseau à l'aide de sous-réseaux, nous sommes limités par le schéma d'adressage IP. Dans certains cas, nous pouvons regrouper des ordinateurs en segments indépendants de leurs adresses IP. Pour ce faire, nous pouvons utiliser des commutateurs et configurer un réseau local virtuel (LAN virtuel ou VLAN). Nous créons un VLAN en associant les hôtes d'un VLAN spécifique à une balise (identificateur d'un VLAN spécifique). Le

protocole de marquage spécifié dans 802.1Q est le protocole de marquage le plus couramment utilisé. Les VLANs fonctionnent à la couche 2 du modèle OSI. Un hôte qui n'a pas de balise est associé au VLAN par défaut, VLAN 1. En isolant les ordinateurs d'un réseau dans des VLAN distincts, nous limitons le domaine de diffusion. La communication entre les VLANs doit se faire via un routeur. Étant donné que nous affectons un hôte à un VLAN via un logiciel, la configuration peut être basée sur les exigences réelles de transfert de données au sein de l'organisation. Par exemple, on peut créer un VLAN séparé pour le service de comptabilité, pour communiquer avec les membres du service de comptabilité, les ordinateurs dans d'autres VLAN de service devraient envoyer des demandes via un routeur et être soumis à toutes les mesures de sécurité de couche 3, telles que les firewalls.

Comme toutes les mesures de sécurité, un VLAN a des vulnérabilités potentielles. Un type d'attaque, appelé sauts VLAN, permet à un attaquant de contourner la frontière VLAN en modifiant l'ID VLAN (balise) sur un paquet. Un attaquant peut également sauter vers un autre VLAN en accédant à un port natif [1].

II.8.2. Utilisation du filtrage des adresses IP et des paquets IP :

En tant que couche de protection supplémentaire, nous devons activer le filtrage sur nos serveurs. Il existe deux types de filtres que nous pouvons appliquer à notre serveur : Filtrage des adresses IP et filtrage des paquets IP.

- **Le filtrage des adresses IP** implique le filtrage du trafic en fonction de l'adresse IP de l'ordinateur client. Certaines applications de serveur Web, comme les services Internet (IIS), nous permettent de filtrer les demandes qu'elles acceptent en fonction de l'adresse IP d'un client. Par exemple, la configuration de la figure II.4 : permet uniquement les connexions à partir du sous-réseau 192.168.10.0 et convient pour un site intranet. Une autre façon de filtrer le trafic en fonction de l'adresse consiste à installer et configurer un firewall personnel.

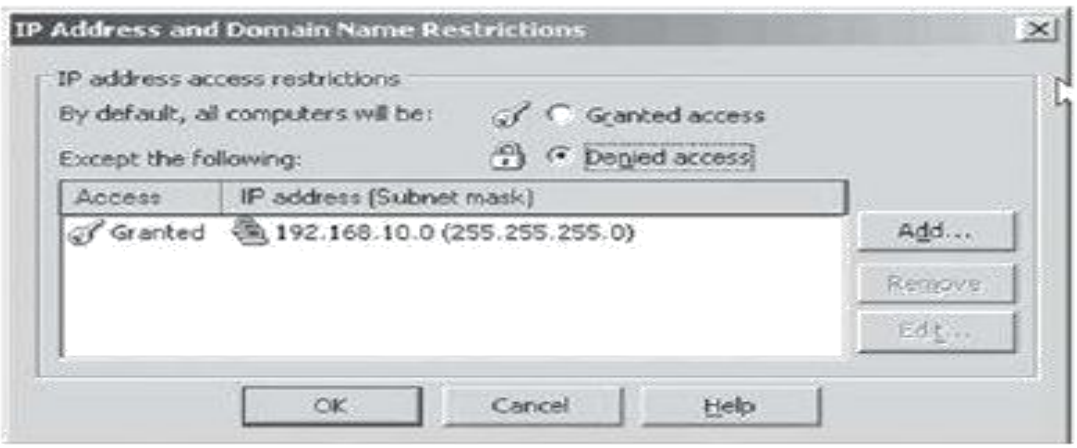


Figure II.6 : Refus d'accès à l'aide du filtrage d'adresses IP [1].

- **Filtrage des paquets IP**

Si nous avons besoin d'un niveau de contrôle supérieur à celui disponible en empêchant une adresse IP de communiquer avec notre serveur, nous pouvons utiliser le filtrage des paquets IP. Le filtrage des paquets IP empêche des paquets spécifiques d'atteindre leurs ports cibles sur le serveur. Cela peut être efficace pour protéger contre les paquets pour des services spécifiques qui ne représenteraient pas le trafic légitime vers le serveur. Nous définissons un filtre en fonction des protocoles ou des numéros de port.

II.9. Sécurisation de la transmission par réseau :

Nous pouvons réduire les risques liés à la transmission de données qui doivent être sécurisées en chiffrant les données, en authentifiant l'utilisateur et en signant les données.

II.9.1. Chiffrement :

En cryptographie, le cryptage est le processus d'encodage de messages ou d'informations de telle manière que seules les parties autorisées peuvent les lire. Le chiffrement n'empêche pas en soi l'interception, mais refuse le contenu du message à l'intercepteur. Dans un schéma de chiffrement, le message ou l'information, appelé texte brut, est chiffré à l'aide d'un algorithme de chiffrement, générant du texte chiffré qui ne peut être lu qu'en cas de déchiffrement. Pour des raisons techniques, un schéma de chiffrement utilise généralement une clé de chiffrement pseudo-aléatoire générée par un algorithme. Un destinataire autorisé peut facilement déchiffrer le message avec la clé fournie par l'expéditeur aux destinataires, mais pas aux intercepteurs non autorisés.

II.9.1.1. Schéma cryptographique de base :

Avant de commencer, nous définissons certains termes. Un message d'origine est appelé *texte brut*, tandis que le message codé est appelé *texte chiffré*. Le processus de conversion du texte brut en texte chiffré est connu sous le nom de *chiffrement* ; la restauration du texte en clair à partir du texte chiffré c'est *déchiffré*. Les nombreux systèmes utilisés pour le chiffrement constituent le domaine d'étude connu sous le nom de *cryptographie*. Un tel schéma est connu comme un système cryptographique ou un chiffrement. Les techniques utilisées pour déchiffrer un message sans connaître les détails de chiffrement relèvent de la cryptanalyse. *Cryptanalysis* est ce que le profane appelle — casser le code —.

Les domaines de la cryptographie et de la cryptanalyse ensemble sont appelés *cryptologie*.

Un algorithme de chiffrement est utilisé pour convertir du texte en clair en texte chiffré, et inversement. Les algorithmes de chiffrement s'appuient souvent sur un mécanisme appelé clé,

de sorte que la relation entre un texte brut et le texte chiffré dépend à la fois de l'algorithme et de la valeur de la clé.

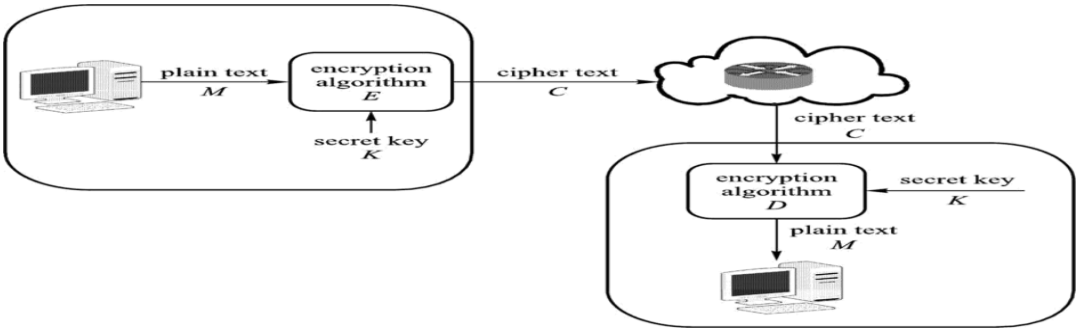


Figure II.7 : Un schéma cryptographique de base [3].

II.9.1.2. Classification des crypto-systèmes :

Les systèmes cryptographiques sont caractérisés par trois dimensions indépendantes :

- **Type d'opérations utilisées pour la transformation du texte brut en texte chiffré :** Tous les algorithmes de chiffrement sont basés sur deux principes généraux : substitution, dans laquelle chaque élément du texte brut (bit, lettre, groupe de bits ou lettres) est mappé à un autre élément, et transposition, dans laquelle les éléments du texte brut sont réorganisés. L'exigence fondamentale est qu'aucune information ne soit perdue (c'est-à-dire que toutes les opérations sont réversibles).
- **Nombre de clés utilisées :** Si l'expéditeur et le destinataire utilisent la même clé, le système est appelé cryptage symétrique, à clé unique, à clé secrète ou conventionnel. Si l'expéditeur et le destinataire utilisent des clés différentes, le système est appelé chiffrement asymétrique, à deux clés ou à clé publique.
- **Mode de traitement du texte brut :** Un chiffrement par bloc traite l'entrée un bloc d'éléments à la fois, produisant un bloc de sortie pour chaque bloc d'entrée. Un cryptage de flux traite les éléments d'entrée en continu, produisant un élément à la fois, au fur et à mesure.

II.9.1.2.1. Système à clé symétrique :

Le cryptage symétrique, également appelé cryptage conventionnel ou cryptage à clé unique, était le seul type de cryptage utilisé avant le développement du cryptage à clé publique dans les années 1970. Il reste de loin le plus utilisé des deux types de cryptage. La même clé est utilisée pour le chiffrement et le déchiffrement ou une clé est simplement dérivée de l'autre, cette clé est appelée la clé secrète ou la clé privée. En utilisant le cryptage symétrique, seuls l'expéditeur et le destinataire connaissent la clé, qui peut être transmise via un canal sécurisé,

par exemple en personne, sur un réseau crypté, etc. Tant que la clé reste secrète, elle fournit également l'authentification prouvant ainsi l'identité de l'expéditeur.

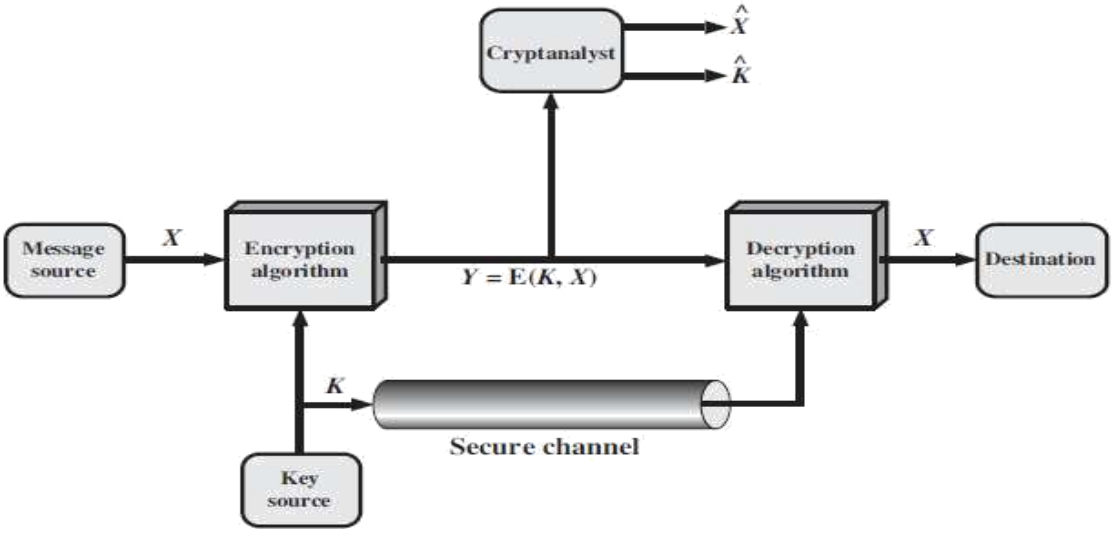


Figure II.8 : Cryptage symétrique [5].

Inconvénients du chiffrement symétrique des clés

Il est difficile d'assurer la sécurité du canal sur lequel la clé est transmise. Parce que lorsque deux parties sur un réseau souhaitent communiquer, elles doivent échanger des clés secrètes en utilisant un canal sécurisé, mais comment peut-on établir un canal chiffré sécurisé sur lequel la clé doit être partagée si l'établissement d'un canal sécurisé nécessite que les deux parties aient déjà des clés secrètes, ce dilemme est appelé le problème d'échange de clés.

Un grand nombre de clés uniques sont nécessaires pour permettre à un grand nombre de personnes de communiquer en toute sécurité, afin d'assurer la sécurité, une clé distincte est nécessaire pour chaque paire expéditeur/récepteur communicant, pour N utilisateurs communicants, nous aurions donc besoin : N*(N-1)/2 touches. Une infrastructure de distribution efficace est donc nécessaire.

II.9.1.2.2. Système à clé asymétrique :

Cette méthode de chiffrement est également connue sous le nom de système de clé publique (PKE), où une clé est utilisée pour le chiffrement, tandis qu'une clé très différente est utilisée pour le déchiffrement. La clé de chiffrement est appelée la clé publique, tandis que la clé de déchiffrement est appelée la clé privée. Les systèmes d'échange de clés publiques éliminent les problèmes rencontrés avec les systèmes de clés symétriques.

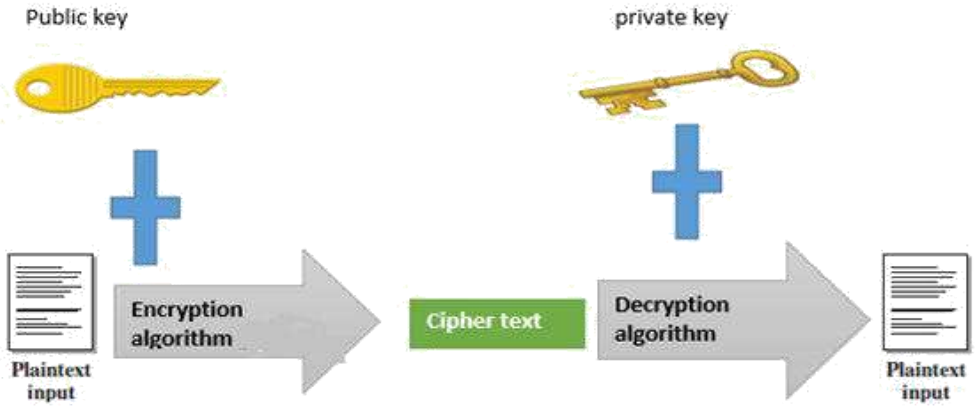


Figure II.9 : Système à clé asymétrique.

II.9.1.3. Distribution des clés dans un système PKE :

Le récepteur crée une clé de cryptage (publique) et sa clé de décryptage associée (privée) où les deux clés sont totalement différentes l'une de l'autre. Le récepteur distribue ensuite la clé publique à quiconque veut lui envoyer des messages chiffrés, il n'est pas nécessaire d'envoyer la clé publique sur un canal sécurisé car seule la clé privée peut décoder le message. L'expéditeur chiffre le message à l'aide de la clé publique et l'envoie au destinataire, seul le destinataire peut le décoder car il est le seul à avoir la clé privée.

Les crypto-systèmes asymétriques permettent des transactions de données sécurisées sur Internet en résolvant les problèmes des systèmes à clé symétrique, malheureusement son rythme de 10000 fois plus lent que le cryptage symétrique, c'est pour cette raison que le cryptage symétrique sert de véritable cheval de bataille pour la communication sécurisée sur Internet

I.9.2. Hachages :

La dernière primitive de la cryptographie est les fonctions de hachage. Les fonctions de hachage sont utilisées pour améliorer les performances lors de la signature de grands blocs de données à l'aide d'un chiffrement asymétrique, pour assurer l'intégrité, dans les protocoles d'authentification et pour créer des données pseudorandom.

II.9.2.1. Fonctions de hachage :

Une fonction de hachage prend un message de n'importe quelle taille et calcule un message plus petit et de taille fixe appelé un résumé ou un hachage. Un exemple de fonction de hachage propriétaire est l'algorithme Message-Digest 5 **(**MD5**)**.

La façon dont ces fonctions de hachage calculent un résumé à partir d'un message arbitrairement volumineux dépasse notre portée, mais il y a trois propriétés de toutes les fonctions de hachage qui les rendent très utiles.

- Il est impossible de trouver deux messages qui peuvent être hachés dans le même résumé.
- Compte tenu d'un résumé, il est impossible de trouver un second message qui créera le même résumé.
- Compte tenu d'un résumé, il est impossible de trouver le message d'origine qui a créé ce résumé.

II.9.3. Signatures numériques :

Une signature numérique est un schéma mathématique permettant de démontrer l'authenticité d'un message ou d'un document numérique. Une signature numérique valide donne au destinataire une raison de croire que le message a été créé par un expéditeur connu, de sorte que l'expéditeur ne peut pas nier avoir envoyé le message **(**Authentification et non-répudiation**)** et que le message n'a pas été modifié en transit (intégrité). Les signatures numériques sont couramment utilisées pour la distribution de logiciels, les transactions financières, et dans d'autres cas où il est important de détecter la falsification.

Les signatures numériques utilisent la cryptographie asymétrique**.** Une signature numérique crypte un message avec une clé privée afin que tout le monde puisse le lire, mais vérifie qu'il provient du détenteur de la clé privée car seule la personne qui détient la clé privée peut créer du texte chiffré qui peut être déchiffré à l'aide de la clé publique.

Utiliser un chiffrement asymétrique est vraiment, vraiment lent. Si l'implémentation de la signature numérique chiffrait l'intégralité du fichier, elle serait lente. Pour pallier ce problème, le message est représenté par un message plus petit, signé et envoyé avec le message d'origine non chiffré. Ce message est si petit qu'il ne prend qu'un temps infime à signer. Maintenant, n'importe qui peut lire le message et peut également vérifier qu'il provient vraiment de l'expéditeur et personne d'autre. Nous allons faire ce petit message qui représente le plus grand avec une fonction de hachage.

Les signatures numériques sont équivalentes aux signatures manuscrites traditionnelles à bien des égards, mais les signatures numériques correctement mises en oeuvre sont plus difficiles à forger que le type manuscrit. Les signatures numériques peuvent également fournir

une non-répudiation, ce qui signifie que le signataire ne peut pas prétendre avec succès qu'il n'a pas signé un message, tout en affirmant également que sa clé privée reste secrète ; en outre, certains systèmes de non-répudiation offrent un cachet temporel pour la signature numérique, de sorte que même si la clé privée est exposée, la signature est valide.

Un schéma de signature numérique se compose généralement de trois algorithmes :

- Un algorithme de génération de clé qui sélectionne une clé privée uniformément au hasard à partir d'un ensemble de clés privées possibles. L'algorithme produit la clé privée et une clé publique correspondante.
- Algorithme de signature qui, avec un message et une clé privée, produit une signature.
- Algorithme de vérification de signature qui, à la suite d'un message, d'une clé publique et d'une signature, accepte ou rejette la revendication d'authenticité du message.

II.9.4. Protocoles de protection de la transmission des données :

Plusieurs protocoles sont disponibles pour l'authentification, le chiffrement et la garantie de l'intégrité des données lorsqu'elles sont transmises sur le réseau, notamment SSL, TLS, IPsec, la signature SMB et SSH.

II.9.4.1. SSL et TLS :

SSL et **TLS** sont des protocoles qui assurent le chiffrement et l'intégrité des sessions pour les paquets envoyés d'un ordinateur à un autre. Ils peuvent être utilisés pour sécuriser le trafic réseau client-serveur ou serveur-serveur. Ils fournissent également l'authentification du serveur au client et (éventuellement) du client au serveur par le biais de certificats X.509 (certificats numériques).

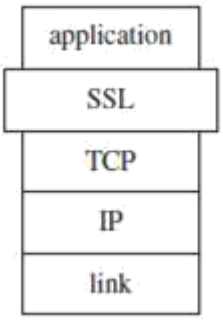


Figure II.10 : Couche de sécurité SSL [2]

L'utilisation la plus courante de SSL est entre un client web et un serveur web parce qu'il est pris en charge par les navigateurs web et les serveurs web sur toutes les plates-formes et est devenu la norme pour chiffrer le trafic HTTP. Cependant, SSL peut également être utilisé pour communiquer avec les serveurs d'applications ou de bases de données, à condition que le système de gestion d'applications ou de bases de données prenne en charge SSL. SSL fonctionne entre les couches Application et Transport de la pile de protocoles réseau, comme indiqué à la figure II.10 ci-dessus.

II.9.4.2. SSH (Secure Shell) :

Les utilisateurs distants s'appuient souvent sur des programmes de connexion distants, tels que rsh, ftp, rlogin, rcp, etc., pour obtenir la connectivité aux machines hôtes pour les besoins des applications. Ces programmes transmettent des données en texte clair. Secure Shell (SSH), géré par l'Internet Engineering Task Force, et traite ce problème avec des programmes de connexion à distance tels que Telnet et ftp. Les services SSH ont une sécurité comparativement plus élevée que les services comme Telnet.

SSH est maintenant disponible en standard pour les connexions à distance. Les applications standard de SSH incluent l'accès à distance aux ressources informatiques via Internet, les transferts de fichiers sécurisés et l'administration système à distance.

II.9.4.3 Sécurité IP (IPsec) :

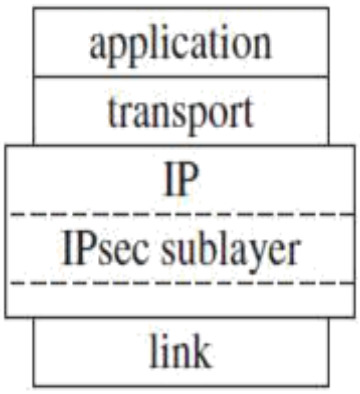


Figure II.11 : Couche IPsec dans la pile de protocoles TCP/IP [2].

IPsec est un protocole de sécurité qui fonctionne sur la couche Internet de la pile de protocoles TCP/IP. Comme il fonctionne sur la couche Internet, il est indépendant des applications. Les applications n'ont pas besoin de prendre en charge IPsec. En fait, ils n'en sont pas du tout conscients.

IPsec inclut deux mécanismes de sécurité principaux, *Authentication Header (AH***),** décrits dans *RFC 2402* et *Encapsulating Security Payload (ESP),* couverts par *RFC 2406,* pour fournir confidentialité et authenticité des paquets IP. L'architecture IPsec est décrite dans *RFC 2401***.** Chaque protocole peut fonctionner dans l'un des deux modes, Transport ou tunnel.

- **En mode transport**, des informations d'en-tête IPsec supplémentaires sont insérées avant les données du paquet d'origine et seule la charge utile du paquet est chiffrée ou authentifiée.
- **En mode tunnel**, un nouveau paquet est construit avec des informations d'en-tête IPsec, et l'ensemble du paquet d'origine, y compris son en-tête, est encapsulé comme charge utile du nouveau paquet

II.9.5. Réseau privé virtuel (VPN) :

Le VPN est une technologie qui permet d'étendre en toute sécurité des réseaux privés sur de longues distances physiques en utilisant un réseau public comme Internet, comme moyen de transport. Les entreprises utilisent généralement des VPN pour permettre l'accès aux utilisateurs distants ou pour connecter plusieurs sites distants. Les entreprises peuvent également utiliser un VPN pour fournir un accès sécurisé aux ressources réseau à leurs clients ou fournisseurs de confiance. Les VPN offrent de meilleures performances que les connexions d'accès à distance car les utilisateurs peuvent tirer parti des connexions Internet haut débit. Les VPN offrent une connectivité entre les bureaux sans le coût de lignes dédiées parce que le trafic traverse l'infrastructure d'Internet. Le mécanisme de protocole le plus courant utilisé à cette fin est au niveau IP et est connu sous le nom IPsec.

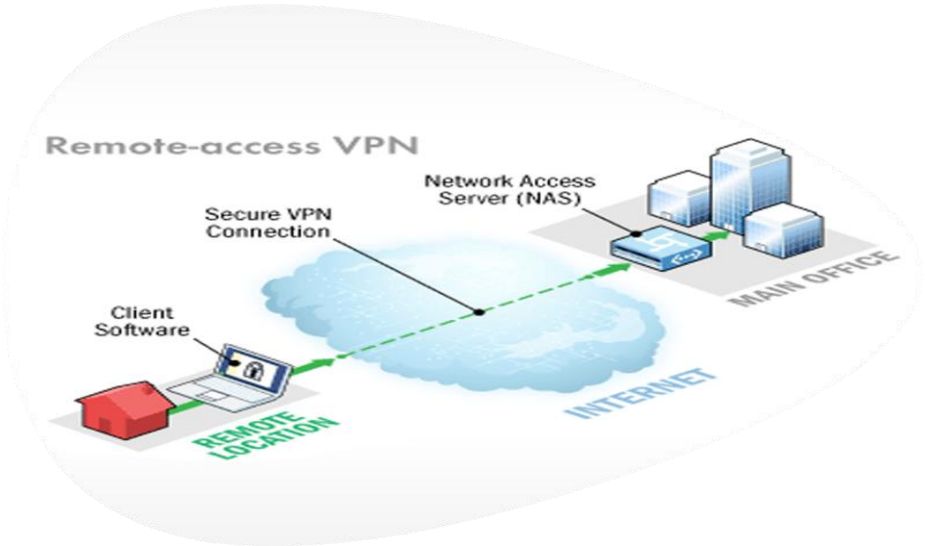


Figure II.12 : Un VPN d'accès à distance [7].

II.9.6. Détection des intrusions et criminalistique :

Même avec des mécanismes de prévention en place, à un moment donné, une attaque se produira. Plus le temps s'écoule entre le début d'une attaque et le moment où vous réalisez qu'une intrusion s'est produite, plus le pirate fera de dégâts. Par conséquent, il est essentiel que vous ayez des systèmes en place pour vous alerter d'une éventuelle attaque.

- **La détection des intrusions :** englobe une variété de catégories et de techniques. Les approches principales consistent à déterminer si un système a été infecté par des virus ou d'autres codes malveillants et à appliquer des méthodes pour détecter une intrusion dans le réseau par un attaquant.
- **Systèmes de détection des intrusions (IDS) :** est un système qui surveille le trafic réseau ou qui vérifie les journaux afin de déterminer si des violations de la politique de sécurité d'une organisation ont été commises. Un IDS peut détecter les intrusions qui ont contourné ou transité par un firewall ou qui se produisent dans le réseau local (LAN) derrière le firewall. Il existe différents types de SID. Les approches les plus courantes en matière de détection des anomalies statistiques (également connues sous le nom de détection basée sur le comportement) et de détection basée sur les signatures (également connues sous le nom de détection basée sur les connaissances ou de détection de modèles).

II.9.7. Systèmes de prévention des intrusions (IPS) :

Un système de prévention des intrusions (IPS) est similaire à un IDS, sauf qu'il détecte et consigne non seulement les tentatives d'intrusion suspectées, mais également les empêche. Un IPS peut être basé sur l'hôte ou sur le réseau. Il peut utiliser des signatures d'attaques ou des anomalies comme base pour bloquer le trafic. L'un des inconvénients potentiels d'un IPS est que les faux positifs empêchent le trafic réseau légitime

II.10. Modèle de sécurité de base :

Le modèle de sécurité de base comprend quatre composantes : les cryptosystèmes, les firewalls, les systèmes logiciels anti-programmes malveillants (logiciels AMS) et les systèmes de détection des intrusions (systèmes IDS). Les cryptosystèmes utilisent la cryptographie informatique et les protocoles de sécurité pour protéger les données. Les protocoles de sécurité comprennent les protocoles de chiffrement, les protocoles d'authentification et les protocoles de gestion des clés.

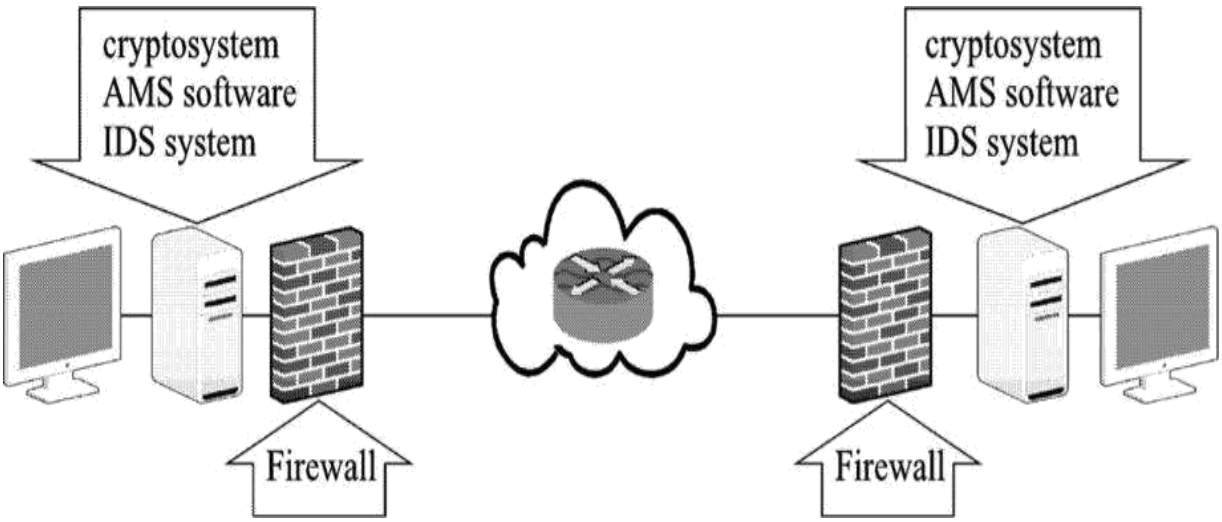


Figure II.13 : Modèle de sécurité de base [3].

Les firewalls, les logiciels AMS et les systèmes IDS sont utilisés pour protéger les données stockées sur les ordinateurs en réseau. Les firewalls sont des progiciels spéciaux installés dans les ordinateurs et les périphériques réseau qui vérifient les paquets réseau entrants et sortants. Certaines caractéristiques des firewalls ont également été incorporées dans les périphériques matériels pour atteindre des vitesses de traitement plus rapides. Le logiciel AMS analyse les répertoires, fichiers et registres système pour identifier, mettre en quarantaine ou supprimer le code malveillant. Les systèmes IDS surveillent les connexions système, étudient les comportements des utilisateurs et analysent les fichiers journaux pour identifier et émettre des alertes lorsque des intrusions sont détectées.

II.11. Conclusion :

L'utilisation réussie d'un firewall dépend de la sélection d'un produit approprié. Une examine approfondie de l'architecture protégée et de ses vulnérabilités doit être effectuée pour un établissement efficace du firewall.

Les firewalls à filtrage de paquets acceptent ou refusent les paquets sur la base de nombreuses règles qui dépendent des ports source et goal des paquets et d'autres critères. Ce sort de firewall est l'option la plus proche d'un arrangement de firewall prête à l'emploi, mais il est aussi généralement le plus facile à déjouer. Les firewalls basés sur un proxy, tels que les firewalls à passerelle de circuit, sont généralement plus difficiles à déjouer, et l'association de circuit virtuel qui en résulte est de loin relativement transparente pour les utilisateurs. Cependant, les firewalls de sort circuit-gateway ne comprennent pas la sémantique des applications et manquent donc d'une certaine granularité de contrôle.

Les firewalls de passerelle d'application sont également basés sur un proxy, mais ils connectent un client spécifique à une application spécifique. Les firewalls de passerelle d'application peuvent fournir une plus grande granularité de contrôle, mais urgent que chaque application que les proxies atteignent soit modifiée, et ils sont généralement moins transparents pour les utilisateurs que les firewalls de circuit-gateway.

Figure II.14 : Comparaison des technologies des firewalls en termes de sécurité et de rapidité.

CHAPITRE III

Filtrage Web sur Firwall Fortigate (Cas Pratique)

III.1. Introduction :

Dans la politique des entreprises, certaines applications et sites web ne sont pas accessibles pour la majorité de leurs employés pour des raisons et des exigences internes.

Dans notre cas, nous allons appliquer ce filtrage sur un firewall de type fortigate en bloquant certains sites web ainsi que des applications, et par la suite effectuer des tests d'acceptance.

III.2. Le choix du matériel :

Nous allons effectuer notre LAB sur un firewall de type Fortigate 200E :

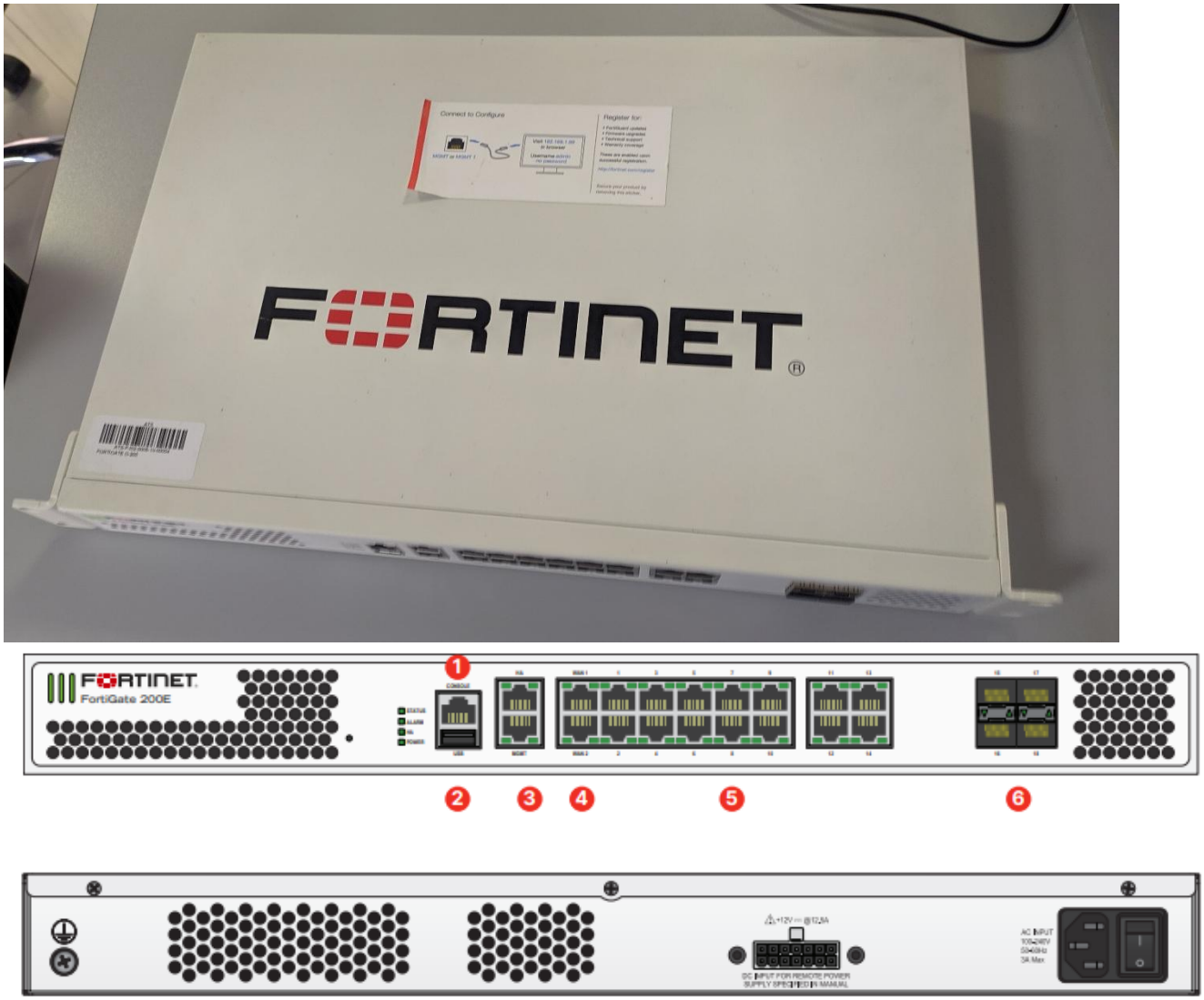


Figure III.1 : Fortigate 200^{E}

- **Interface :**

  1. Console Port.
  2. USB Port.
  3. 2x GE RJ45 MGMT/HA Ports.
  4. 2x GE RJ45 WAN Ports.
  5. 14x GE RJ45 Ports.
  6. 4x GE SFP Slots.

- **Caractéristiques :**

  Débit du firewall : 20000 Mbit/s.

  Débit du VPN : 9000 Mbit/s.

  Débit IPS/IDS: 6000 Mbit/s.

  Utilisateurs simultanés : 300 utilisateurs.

  Niveau sonore : 65 dB.

  Nombre d'utilisateurs : 300 utilisateurs.

  Firewall de sécurité : UDP.

  Support de VPN : IPsec, SSL.

  Programme de gestion : FortiOS

  Et pour la configuration et l'établissement des tests, nous allons utiliser notre LAPTOP.

III.3. La création de « Firewall Policy », « Application Control » et « Web Filter » :

Nous résumons les étapes de configuration et paramétrage comme suit :

Se connecter au Fortigate via le navigateur (Google Chrome, Mozilla Firefo, etc…) en tapant l'adresse IP du firewall tout en introduisant le **nom d'utilisateur** et **mot de passe** :

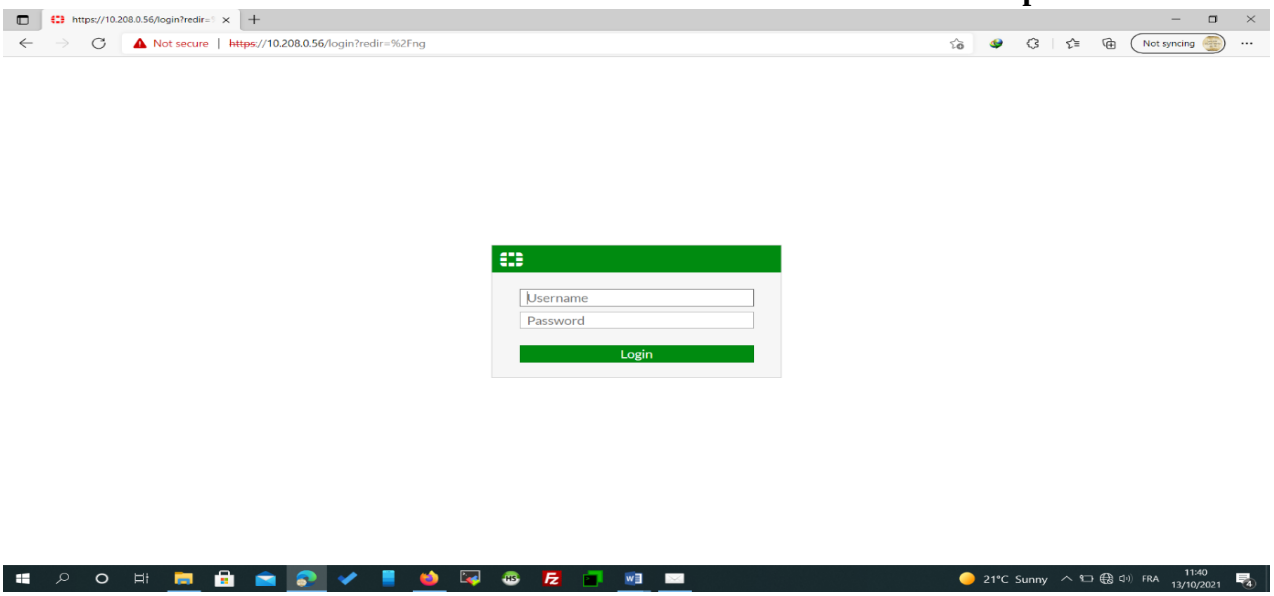


Figure III.2 : Connexion à Fortigate

En connectant, ça nous guide vers la page d'accueil de Fortigate.

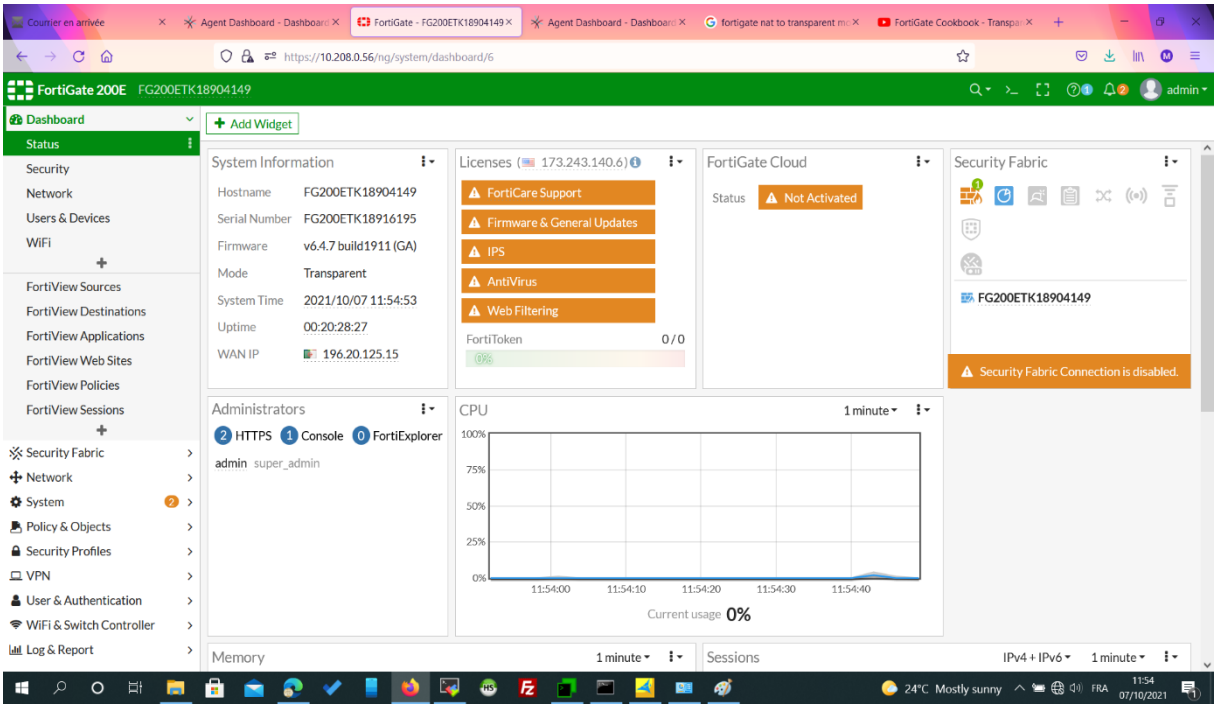


Figure III.3 : Page d'accueil de Fortigate.

III.3.1. Firewall Policy :

Pour créer un profile de Policy, accédez à **Policy & objects > firewall Policy**

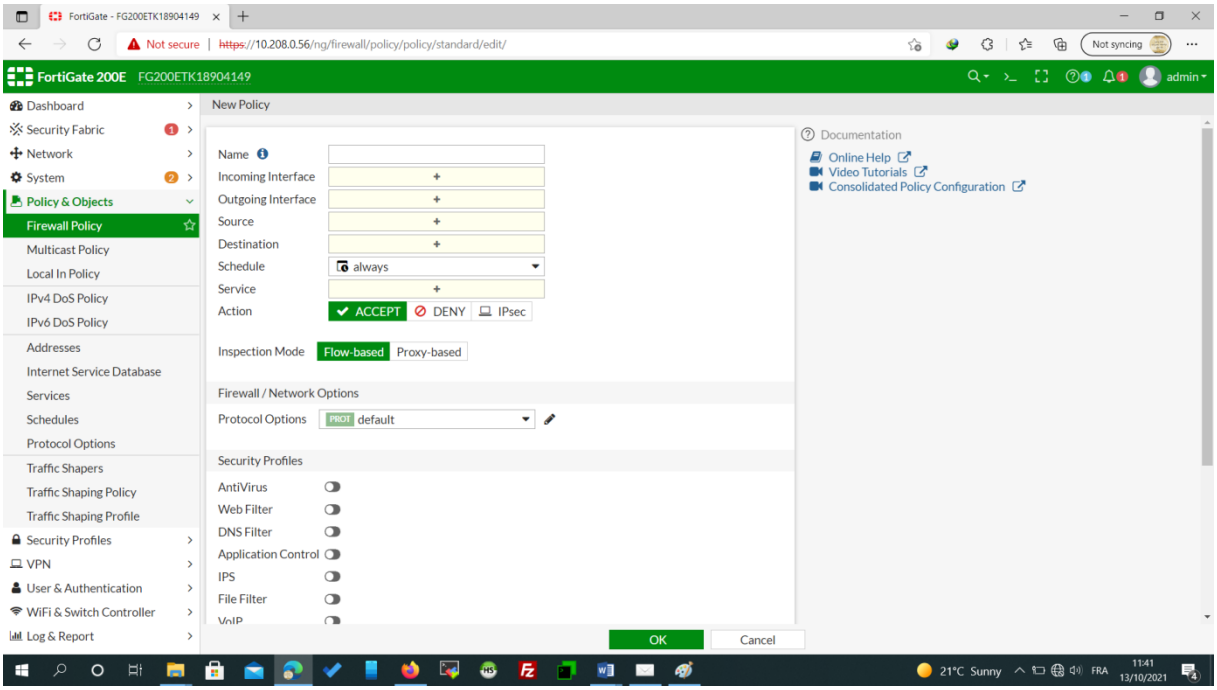


Figure III.4 : Création de Policy.

Nous nommons la nouvelle **policy** « internet-access »

Chaque **policy** a des critères de coordination,que vous pouvez caractériser à l'aide des objets suivants :

- **Incoming Interface :** Peut-être une interface ou une zone.

Il s'agit de l'interface ou des interfaces par lesquelles le trafic est d'abord connecté à l'unité Fortigate. L'exception étant le trafic que le Fortigate génère lui-même. Cela ne se limite pas aux ports

Ethernet physiques trouvés sur l'appareil. L'incoming interface peut également être une interface logique ou virtuelle telle qu'un tunnel VPN, une liaison Virtual WAN ou une interface sans fil.

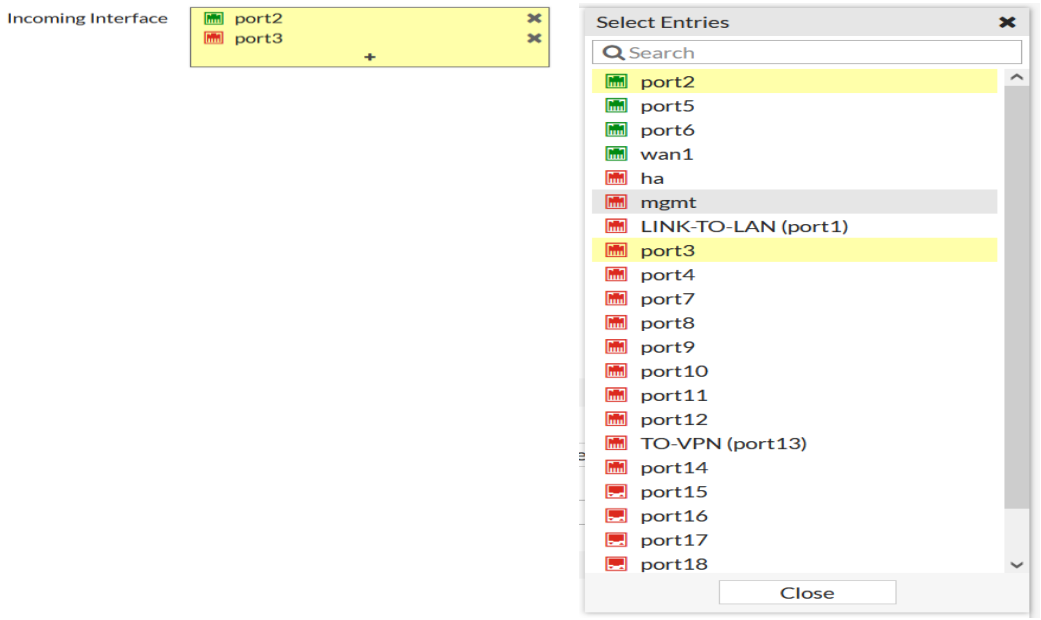


Figure III.5 : Incoming interface.

• **Outgoing Interface :** Peut-être une interface ou une zone.

Une fois que le firewall a traité le trafic, il doit quitter un port pour atteindre sa destination et ce sera l'interface ou les interfaces par lesquelles le trafic quitte. Cette interface, comme l'**incoming interface,** n'est pas limitée aux seules interfaces physiques.

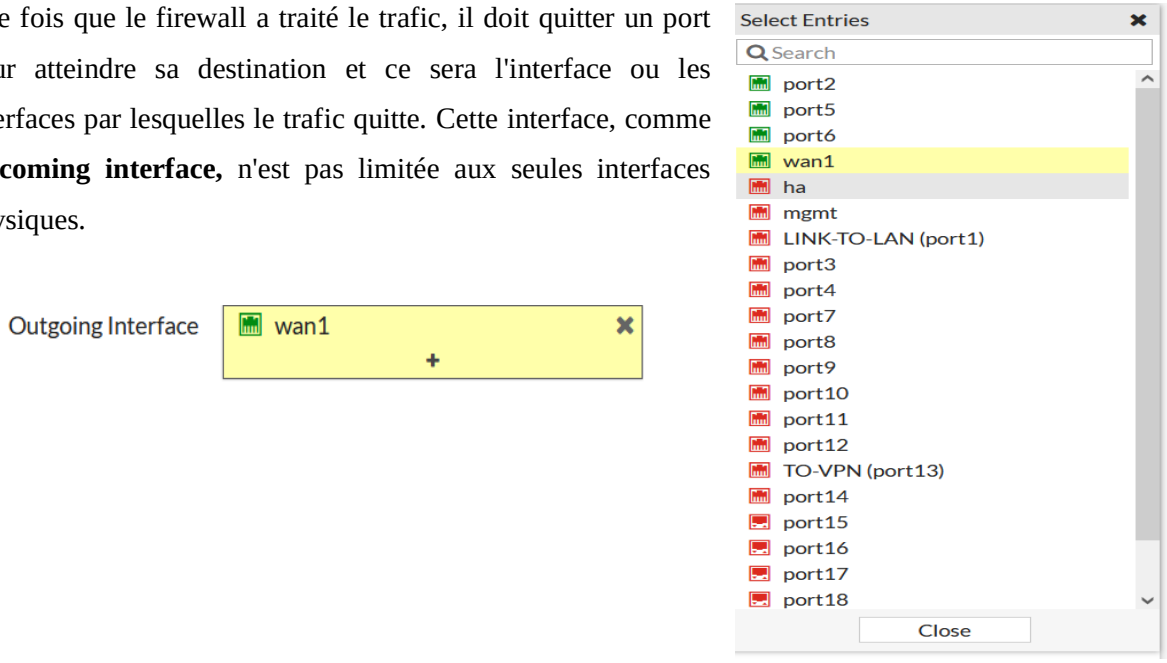


Figure III.6 : Outgoing interface.

Pour correspondre une **policy** à un trafic, nous sélectionnons une (ou plusieurs) interface ou n'importe quelle interface.

• **Source :** Confirme l'identité de l'utilisateur.

L'accès au réseau ne peut être fourni qu'après la confirmation des informations d'identification de l'utilisateur.

Les adresses à partir desquelles une stratégie peut recevoir du trafic peuvent être largement ouvertes ou étroitement contrôlées. Pour un serveur Web public auquel le monde entier devrait pouvoir accéder, le meilleur choix sera « all ».

La destination est un serveur Web privé auquel seules les succursales d'une entreprise devraient pouvoir accéder ou une liste d'ordinateurs internes qui sont les seuls autorisés à accéder à une ressource externe, un groupe d'adresses préconfigurées est la meilleure stratégie.

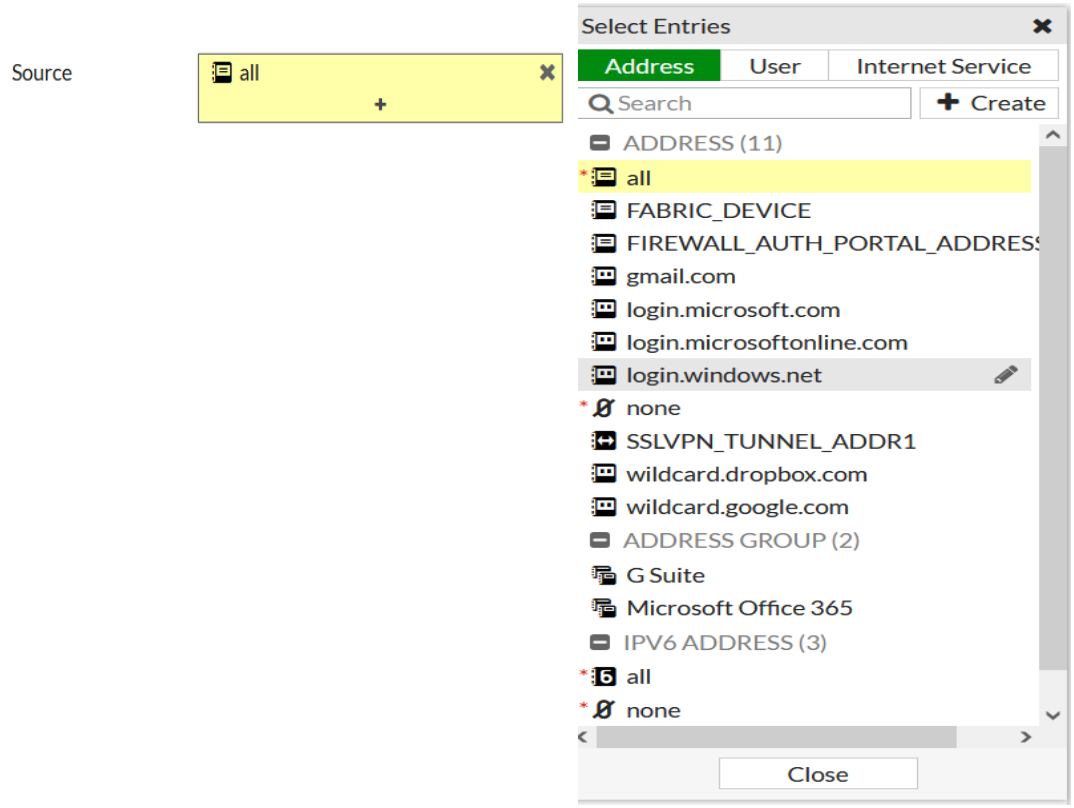


Figure III.7 : Source.

Nous devrons spécifier au moins une source (objet d'adresse ou d'Internet service database «**ISDB**»)

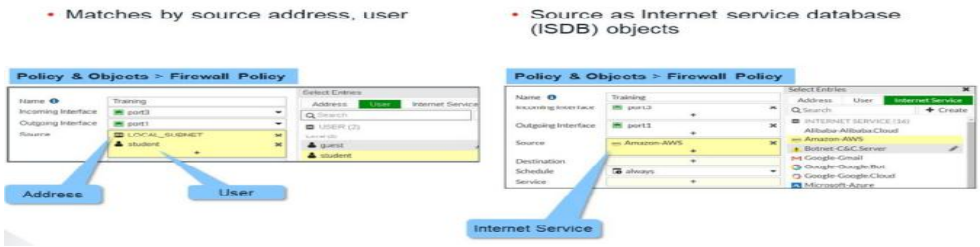


Figure III.8 : Spécification de la source.

Nous pouvons aussi spécifier "**Source User**" (utilisateur individuel ou groupe d'utilisateurs).

Cela peut référer aussi à : - Comptes locaux du firewall

- Comptes sur un serveur distant

• **Destination :** Adresse IP ou services Internet.

Comme la source, le critère de la destination peut utiliser des objets d'adresse ou d'Internet Service Database « **ISDB ».**

De la même manière que l'adresse **source** peut devoir être limitée, l'adresse de destination peut être utilisée comme filtre. Lorsque le trafic est destiné à des ressources internes, l'adresse spécifique de la ressource peut être définie pour mieux protéger les autres ressources du réseau. L'une des options d'adresse de destination spécialisée consiste à utiliser une adresse IP virtuelle. L'adresse de destination n'a pas besoin d'être interne, vous pouvez définir des stratégies qui ne concernent que la connexion à des adresses spécifiques sur Internet

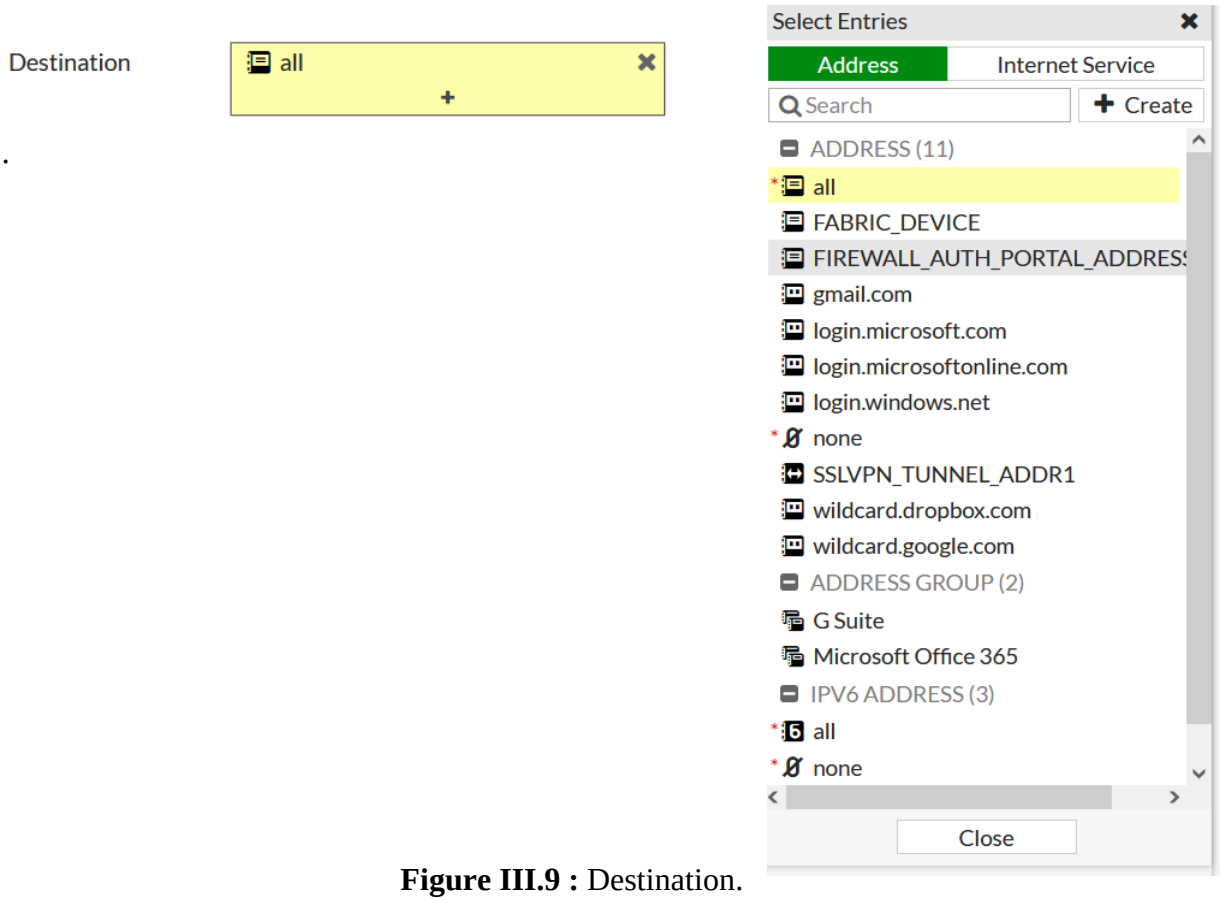


Figure III.9 : Destination.

• **Schedule :** S'applique pendant les périodes configurées.

• **Service :** Protocole IP et numéro de port.

Dans ce contexte, un service est une combinaison d'une ou plusieurs adresses et d'un ou plusieurs services associés à un service présent sur Internet tel qu'un service de mise à jour de logiciels

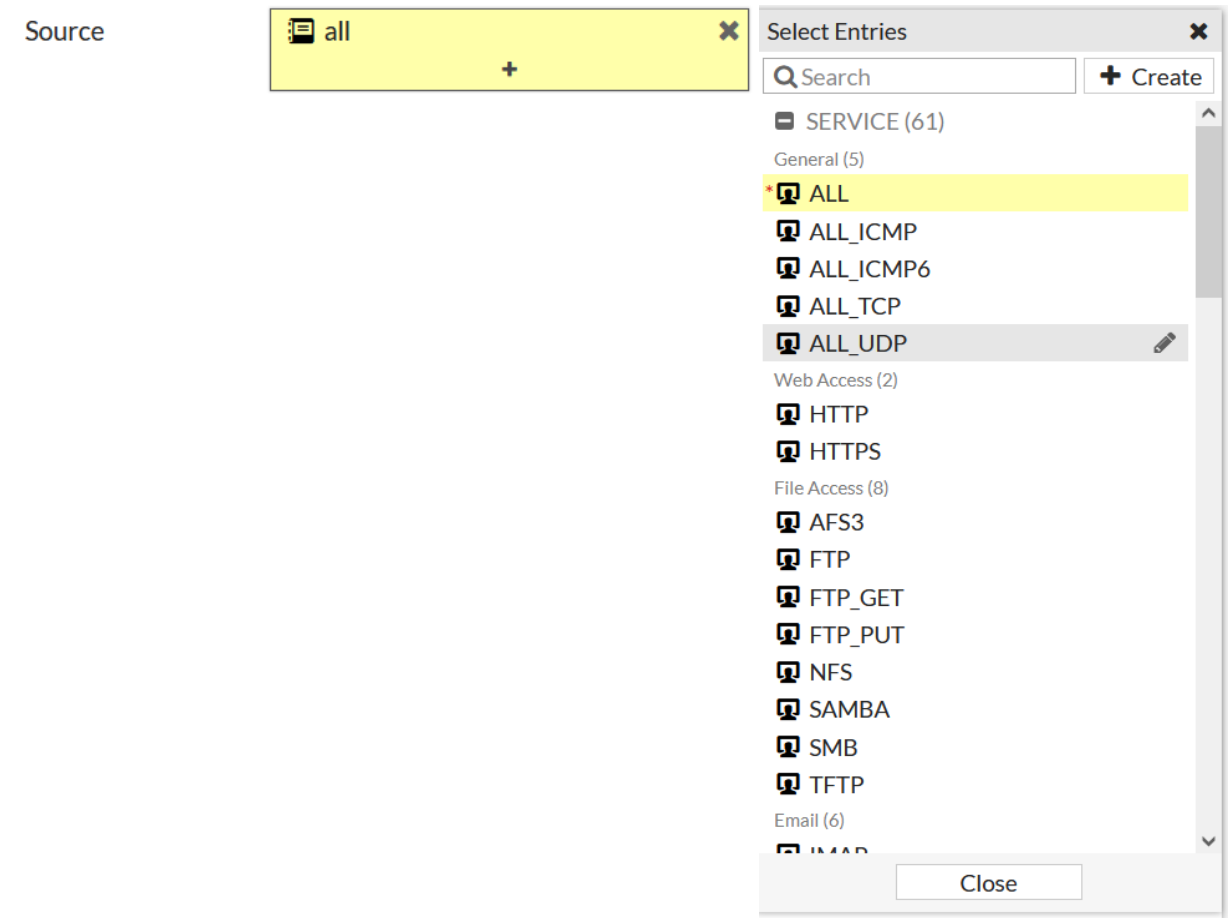


Figure III.10 : Service.

Lorsque le trafic correspond à une policy du firewall, FortiGate applique l'action configurée dans la policy du firewall.

- Si l'action est définie sur **DENY**, FortiGate abandonne la session.

- Si l'action est définie sur **ACCEPT**, FortiGate applique d'autres paramètres configurés pour le traitement des paquets, tels que l'analyse antivirus, le filtrage Web ou le NAT source.

• **Log allowed traffic :**

Dans la plupart des cas, il est recommandé de sélectionner des événements de sécurité, car toutes les sessions nécessitent plus de ressources système et d'espace de stockage. Pour l'instant, cependant, toutes les sessions seront utilisées pour vérifier que la journalisation a été configurée avec succès.

Figure III.11: Log allowed traffic.

III.2. Application control :

FortiGates peut reconnaître le trafic réseau généré par un grand nombre d'applications. Les capteurs d'Application Control spécifient l'action à entreprendre avec le trafic des applications. **Application Control** utilise des décodeurs de protocole **IPS** qui peuvent analyser le trafic réseau pour détecter le trafic des applications, même si le trafic utilise des ports ou des protocoles non standard. **Application Control** prend en charge la détection du trafic à l'aide du protocole **HTTP**.

Fortigate comprend trois capteurs applicatifs préchargés :

- Default (surveille toutes les applications)
- wifi-default (configuration par défaut pour décharger le trafic WiFi)
- block-high-risk

Nous pouveon personnaliser ces capteurs (ou les créer) pour enregistrer et gérer les applications sur notre réseau.

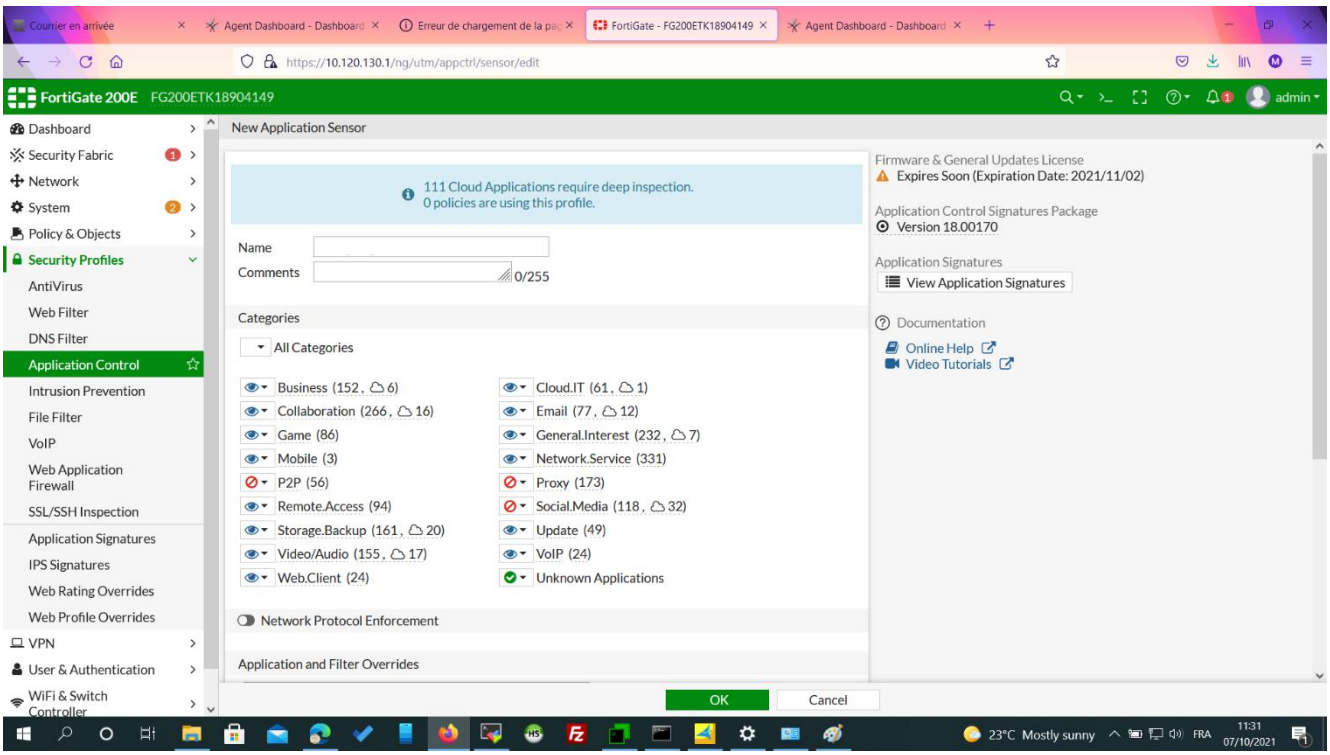


Figure III.12 : Capteurs applicatifs préchargés.

Pour créer un **Application Control** qui définit les applications qu'on souhaite contrôler, nous accédons à **Security Profile > Application Control.**

Nous sélectionnons l'icône **Create New.**

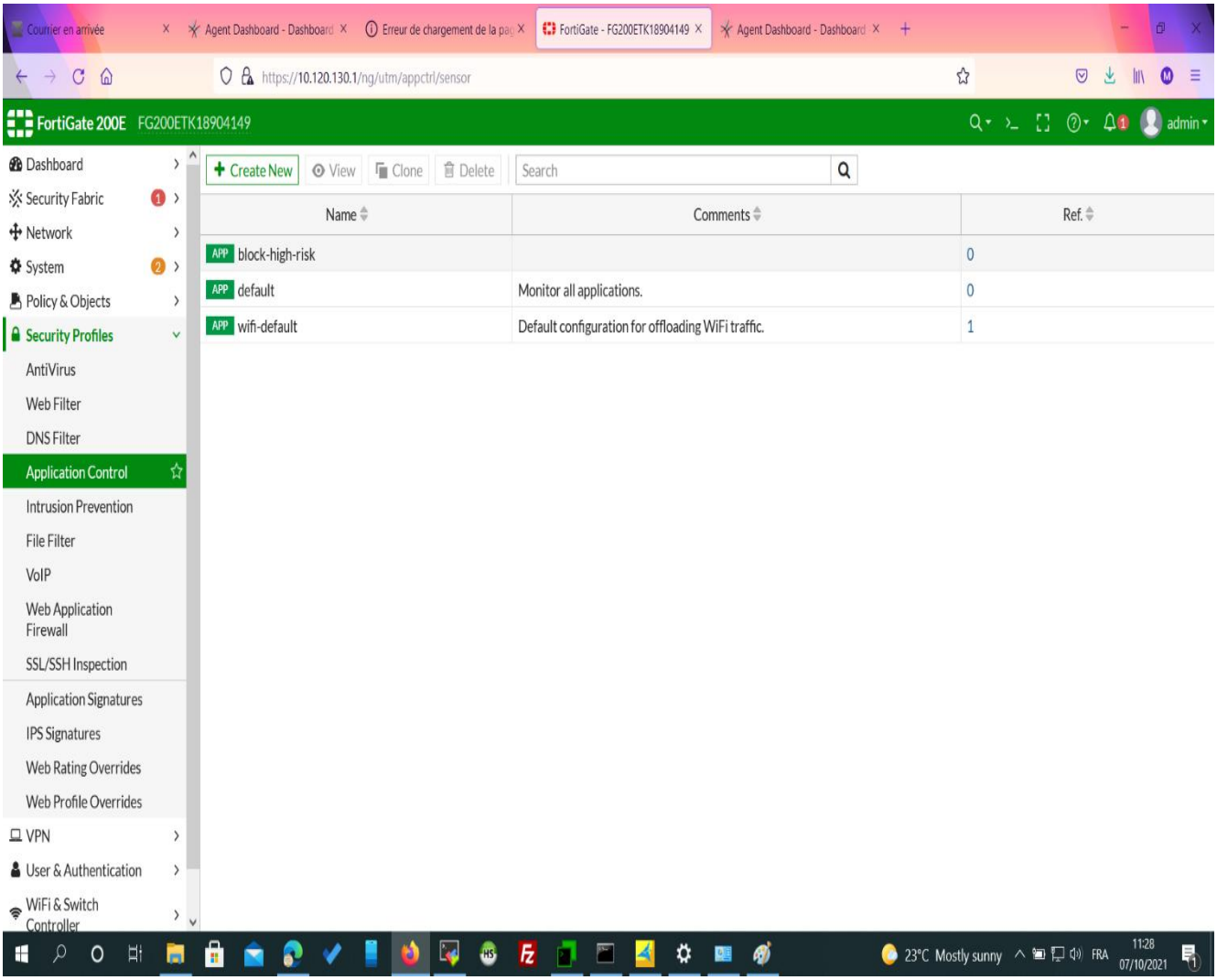


Figure III.13 : Création d'Application Control.

Nous le nommons « **Block_M2_STC »**

Figure III.14 : Nomination de l'Application control

Categories : Les **Categories** nous permettent de choisir des groupes de **signatures** en fonction d'un type de **category**. Les applications appartenant à la **category** déclenchent l'action définie pour cette dernière.

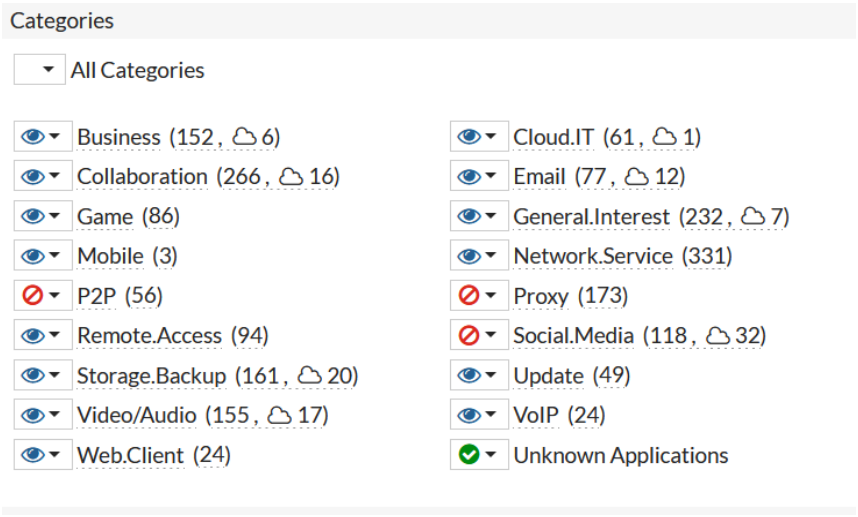


Figure III.15 : Catégories.

Cliquons avec le bouton gauche sur l'icône à côté du nom de la **category** pour afficher une liste déroulante d'**actions**.

Monitor : Autoriser le trafic à continuer vers sa destination et enregistrer son activité

Allow : Autoriser le trafic à continuer vers sa destination

Block : bloquer automatiquement le trafic correspondant à l'une des signatures incluses dans l'entrée.

Quarantine : Permettre de mettre en quarantaine l'adresse IP de l'attaquant pour une durée déterminée (peut-être des jours, des heures ou des minutes …)

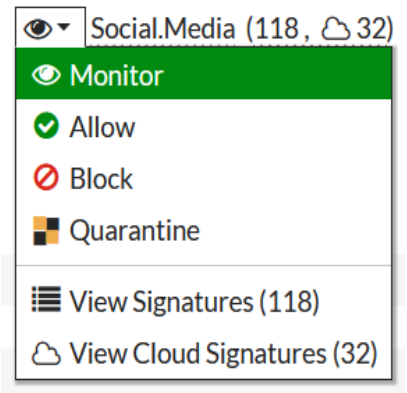


Figure III.16 : Actions.

• Application and filter Overrides :

Nous choisissons une **Application** pour **Application Override.**

Pour créer un **Application Override** nous cliquons sur **Create New** dans la section **Application and filter Overrides**

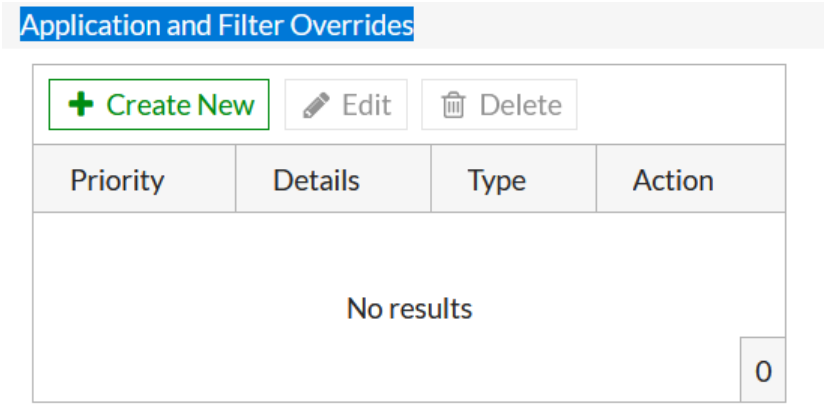


Figure III.17: Application and filter Overrides.

Pour établir un **application override**, nous sélectionnons **Application** comme **type**, et **Block** comme **Action.**

Plusieurs **Application Signatures** peuvent être ajoutées comme une entrée. Un curseur présentant une liste d'applications s'affiche pour sélectionner des signatures d'applications spécifiques, et le champ de recherche peut être utilisé pour filtrer les **Signatures** correspondantes.

Cliquons sur **Add Filter** pour filtrer l'application.

Il suffit de taper le nom de l'application spécifique Youtube et Facebook

Sélectionner les signatures requises.

Cliquez sur **Ok.**

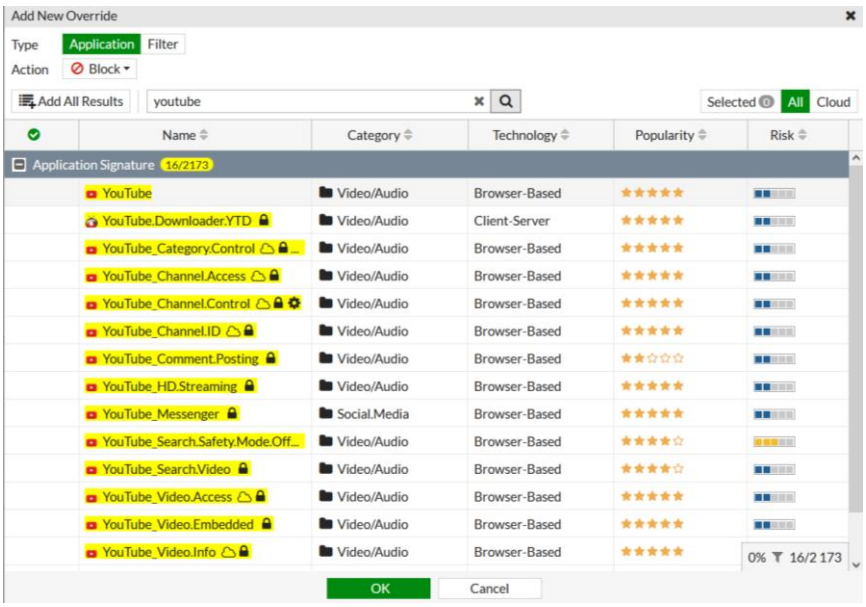


Figure III.18 : Add new Override

En établissant l'**Application Override**, nous achevons un **Application Control** applicable « **Bloc_M2_STC** »

Figure III.19 : Application Control applicable

Pour créer une **security policy** pour l'**Application Control « Bloc_M2_STC »**, nous allons à **Policy & Objects > Firewall Policy**, et nous sélectionnons la **Policy** «**Internet-Access**» ustilisée pour contrôler le trafic.

Nous autorisons l'**Application Control**, puis nous sélectionnons **Bloc_M2_STC** de la liste.

Cliquons sur **Ok.**

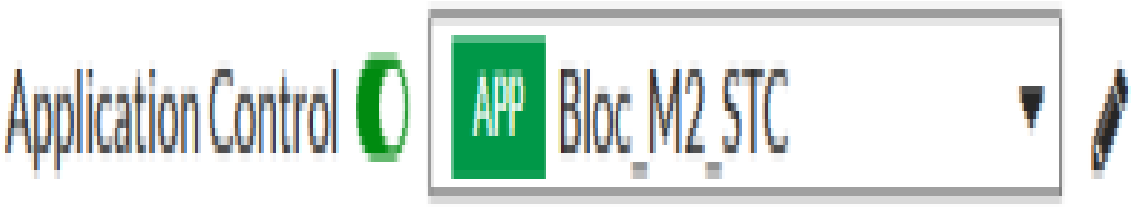


Figure III.20 : L'application d'Application Control dans la Policy « Internet-Access ».

II.3.3. Web filter :

Pour créer un **Web Filter**, nous accédons à **Security Profiles > Web Filter**

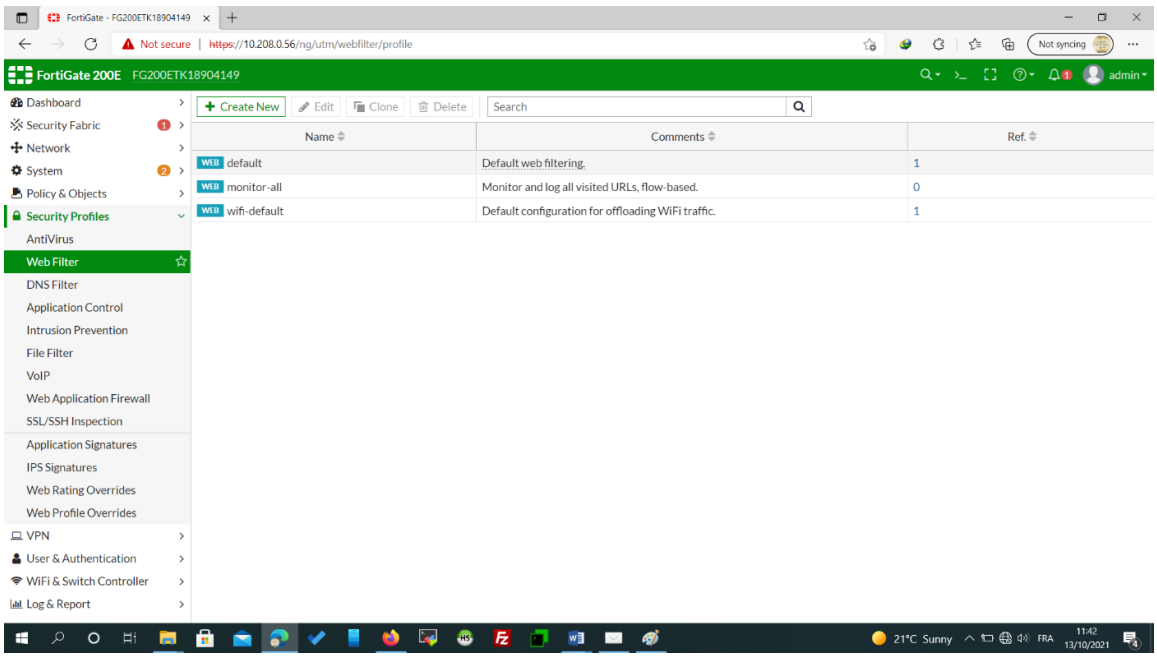


Figure III.21 : Web Filter.

Nous Cliquons sur **Create New,** et nous nommons le Web Filter « **Ticket-Filter** ».

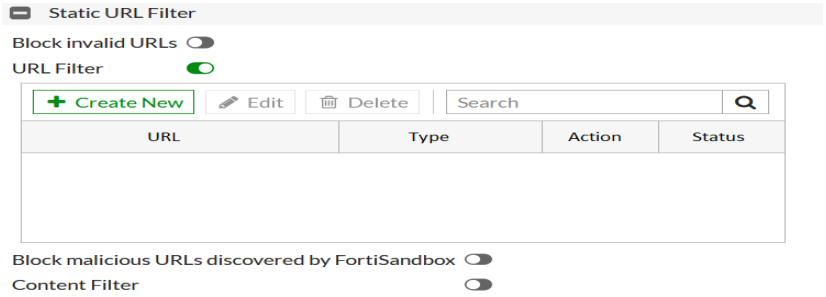


Figure III.22 : Création et nomination de Web Filter

Dans la section de Static URL, nous cochons **Enable URL Filter**, puis nous séléctionnons **Create New**.

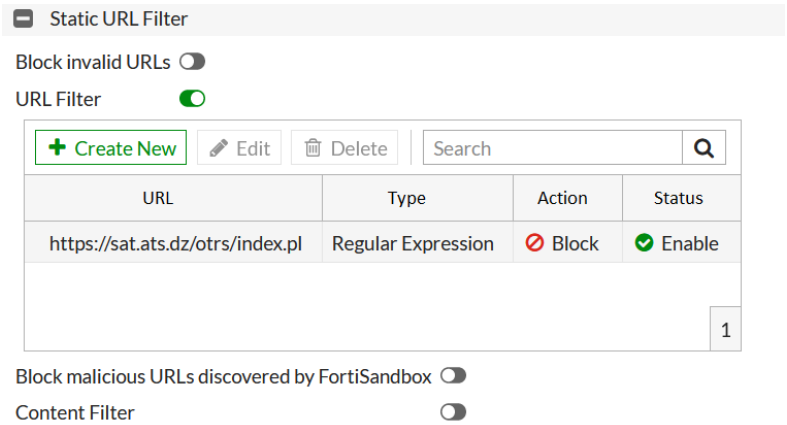


Figure III.23 : Création de l'URL Filter

Pour bloquer le site de l'**ATS**, nous entrons **Https://sat.ats.dz/orts/index.pl** dans le champ **URL,,** puis nous sélectionnons **Regular expression** comme **Type,** et **Block** comme **Action.** Enfin dans le champ **Status**, nous cochons **enable**.

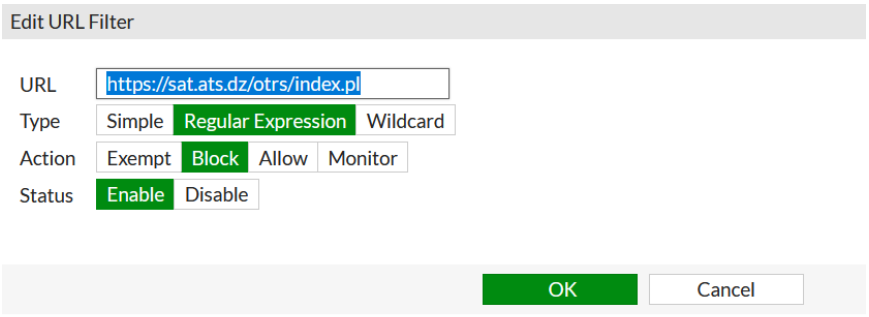


Figure III.24 : Edition de l'URL Filter.

Cliquons sur **Ok**.

Figure III.25 : URL Filter établi.

En établissant l'**URL Filter,** nous achevons un **Web FIlter** applicable.

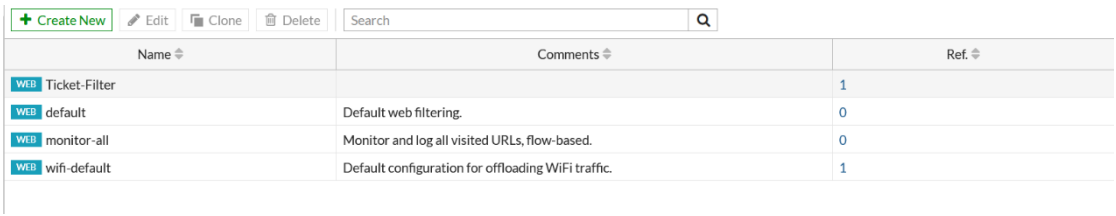
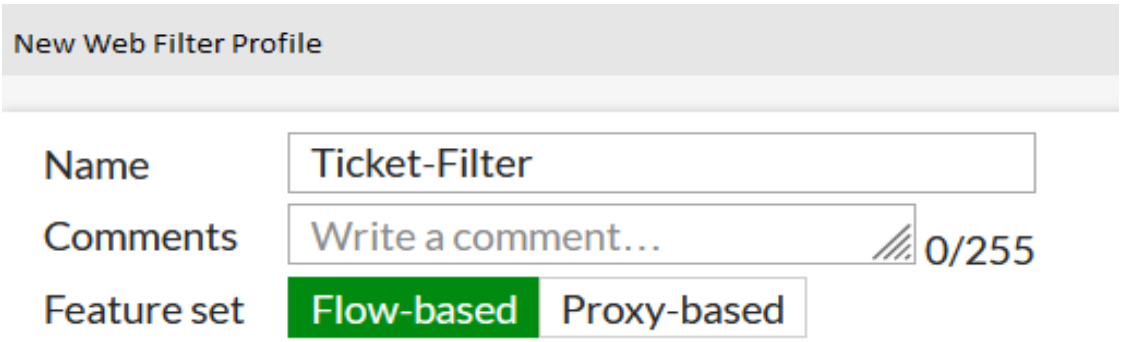


Figure III.25 : Web Filter applicable.



Pour créer une **security policy** pour le **Web Filter « Ticket-Filter »**, nous allons à **Policy & Objects > Firewall Policy**, et nous sélectionnons la **Policy** « **Internet-Access** » utilisée pour contrôler le trafic.

Nous autorisons le **Web Filter**, puis nous sélectionnons **Ticket-Filter** de la liste.

Cliquons sur **OK**.

Figure III.26 : L'application du Web Filter dans la Policy « Internet-Access ».

III.4. Les Tests d'acceptance :

En appliquant la **Policy** avec l'autorisation d'**Application Control**, nous n'arrivons pas à accéder aux applications bloquées, les résultats seront comme suit :

- **Facebook :**

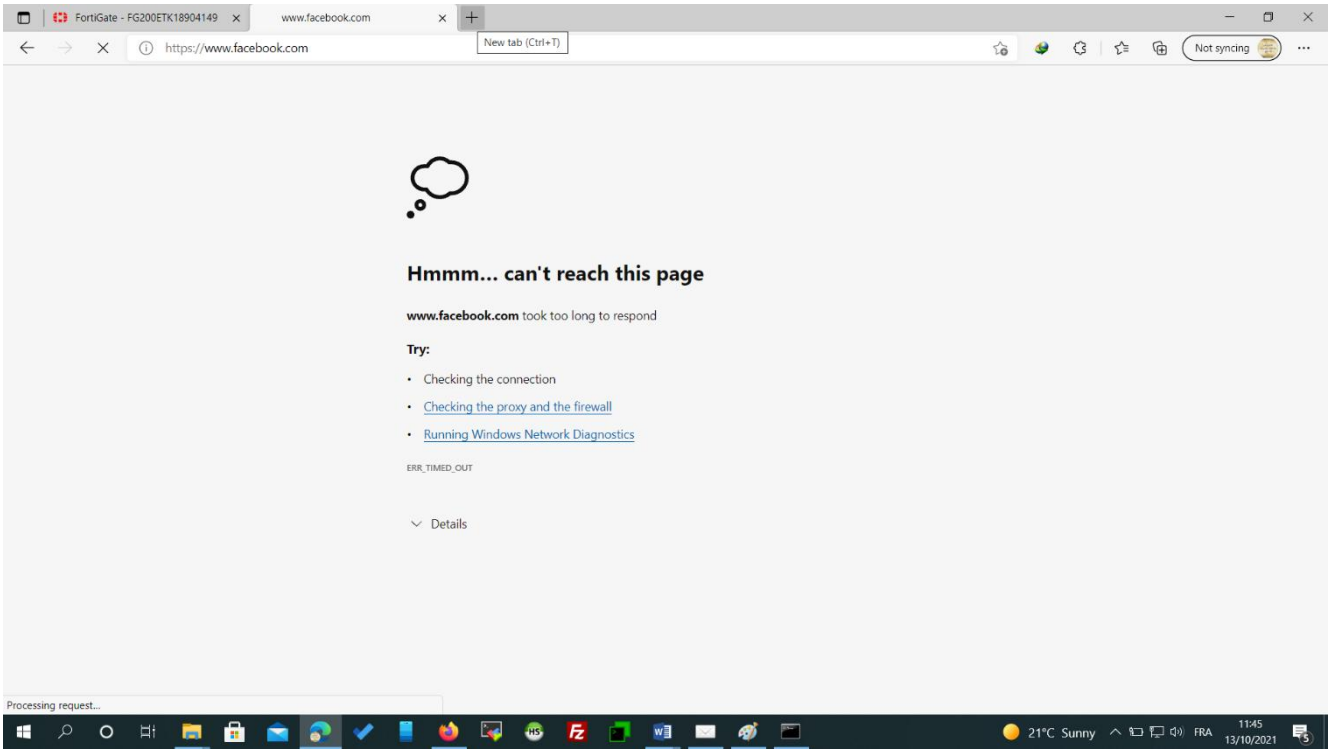


Figure III.27 : Facebook bloqué

- **YouTube:**

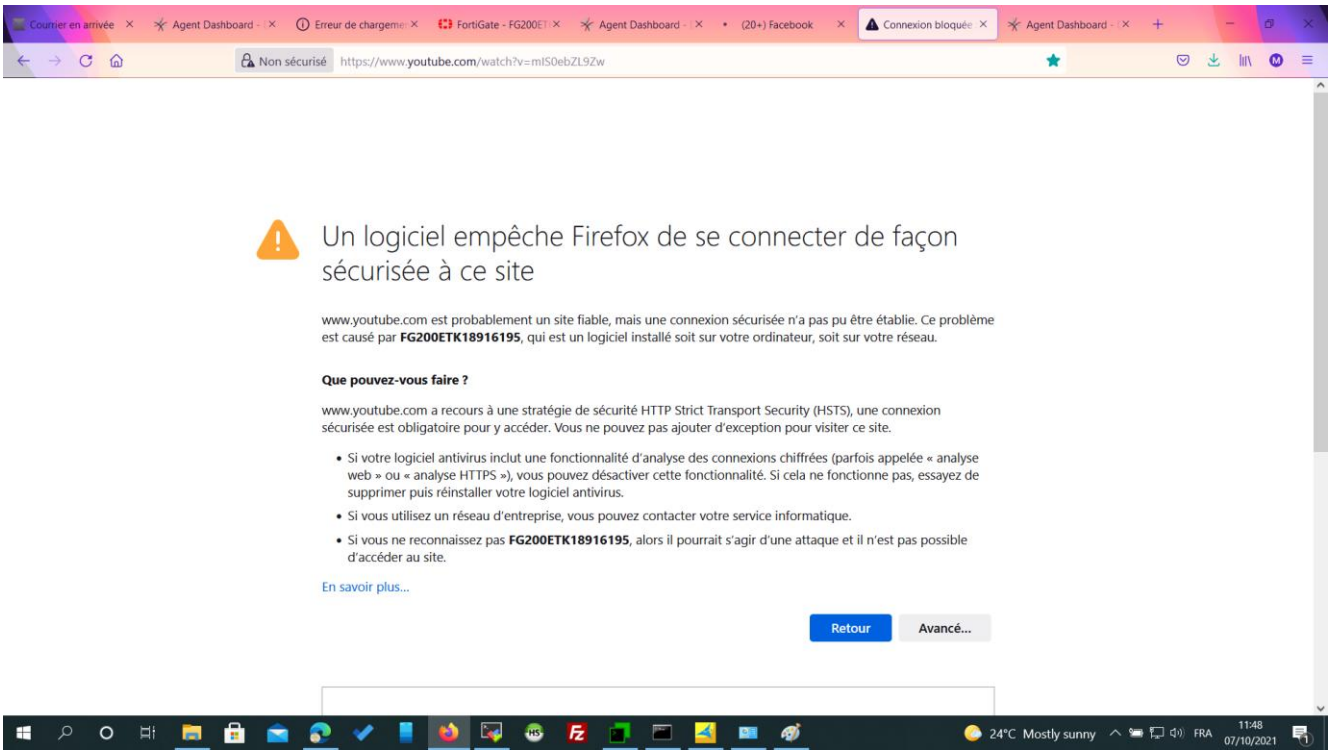


Figure III.28 : YouTube bloqué.

En appliquant la **Policy** avec l'autorisation du **Web Filter**, nous n'arrivons pas à accéder aux applications bloquées, les résultats seront comme suit :

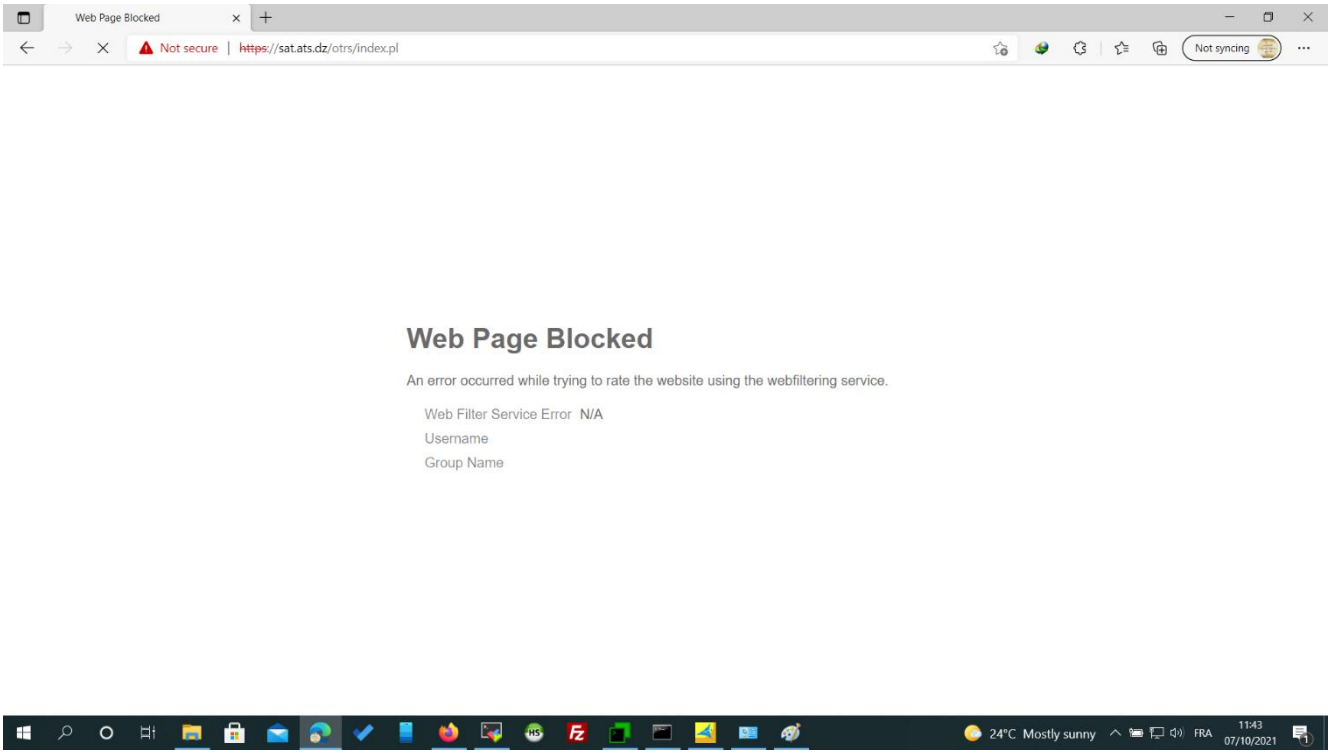


Figure III.29 : Site d'ATS bloqué.

III.5. Conclusion :

Cette partie pratique nous a permis d'établir un test rel sur un firewall de type **Fortigate**, en appliquant des connaissances théoriques acquises.

Notre objectif d'appliquer un filtrage web er applicatif au niveau de firewall était atteint, sachant que les configurations et les tests ont été effectués par nous-même.

Conclusion Générale

Conclusion générale :

La sécurité des réseaux peut être une tâche compliquée. Au fur et à mesure que des mécanismes plus avancés sont créés pour garantir les ressources des réseaux attachées à l'Internet, des efforts similaires sont déployés pour compromettre les instruments de sécurité mis en place. Aucune organisation ne peut prétendre être totalement sécurisée (comme une telle idée est habituelle). Quoi qu'il en soit, une organisation peut prétendre être aussi protégée qu'il est humainement concevable. Les **Security policiers** doivent être continuellement examinés et modifiés. Les systèmes de firewall (matériels et logiciels) doivent être maintenus à jour.

La **sécurité des réseaux** restera un sujet d'interrogation dynamique pour plusieurs raisons. Pour commencer, les mesures de sécurité qui sont fiables aujourd'hui peuvent ne plus l'être demain en raison des progrès et des percées dans les hypothèses de calcul, les calculs et les technologies informatiques. Deuxièmement, une fois les problèmes de sécurité connus résolus, d'autres failles de sécurité qui étaient déjà obscures peuvent à un moment donné être découvertes et utilisées à mauvais escient par les attaquants. Troisièmement, lorsque des applications modernes sont créées ou que des avancées modernes sont concoctées, des problèmes de sécurité non utilisés peuvent en outre être créés avec elles. De cette façon, **la sécurité des réseaux** est implicitement une lutte de longue haleine entre les attaquants et les défenseurs.

Bibliographie

Références:

[1] Network Security Fundamentals - Eric Cole 2007

[2] The Practice of Network Security Monitoring – Lay Flat, August 5, 2013

[3] Computer Network Security Theory and Practice - Jie Wang 2008

[4] Cryptography and Network Security Principles and Practices 5Ed - William Stallings 2011

[5] Cisco ASA All in one Firewall IPS & VPN 2Ed 2010

[6]https://www.paloaltonetworks.com/resources/learning-center/what-is-networksecurity.html (page visited march 2, 2015)

[7] http://en.wikipedia.org/wiki/Network_security (page visited on June 5, 2015)

[8] Davis Chapman, « Firewalls — La sécurité sur Internet », edition O'Reilly, 1997.

[9] http://www.allstateitsolutions.com/network-security/ (page visited on June 8, 2015).

Résumé

La **sécurité des réseaux** est devenue plus importante pour les les utilisateurs d'ordinateurs, les organisations et les militaires. Avec l'avènement d'Internet, la sécurité est devenue une préoccupation majeure. L'histoire de la sécurité permet de mieux comprendre l'urgence des technologies de sécurité. La structure d'Internet elle-même a permis l'apparition de nombreuses menaces pour la sécurité. L'architecture de l'internet, lorsqu'elle est modifiée, peut réduire les attaques possibles qui peuvent être envoyées sur le réseau. En connaissant les méthodes d'attaque, il est possible de mettre en place une sécurité appropriée. De nombreuses entreprises se protègent d'Internet au moyen de **firewalls** et de mécanismes de **cryptage**. Les entreprises créent un "**intranet**" pour rester connectées à l'Internet mais protégées des menaces éventuelles. Le domaine de la sécurité des réseaux est vaste et en pleine évolution. Le champ d'étude englobe un bref historique remontant aux débuts d'Internet et le développement actuel de la sécurité des réseaux. Pour comprendre les recherches menées aujourd'hui, il est nécessaire d'avoir des connaissances de base sur l'internet.

Abstract

Network security has become more important to computer users, Organizations, and the military. With the advent of the Internet, security became a major concern and the history of security allows a better understanding of the emergency of security technology. The Internet structure itself allowed for many security threats to occur. The architecture of the Internet, when modified can reduce the possible attacks that can be sent across the network. Knowing the attack methods, allows for the appropriate security to emerge. Many businesses secure themselves from the Internet by means of firewalls and encryption mechanisms. The businesses create an ―intranet‖ to remain connected to the Internet but secured from the possible threats. The entire field of network security is vast and in an evolutionary stage. The range of study encompasses a brief history dating back to Internet’s beginnings and the current development in network security. In order to understand the research carried out today you need to have background knowledge of the Internet.

ملخص

مع ظهور الأنترنت صبح أمن الشبكات ذو أهمية لمستخدمي الشبكات من حواسيب ومنظمات دولية وغير دولية وكذلك بالنسبة لجيوش العالم أصبح الأمن مصدرا هاما في الحفاظ على البيانات المسجلة خاصة في حالة الطوارئ. وبفضل تكنولوجيا الأمن يتم التقليل من الهجمات المحتملة التي يمكن إرسالها عبر الشبكات . توجد عدة أساليب للهجوم عبر الشبكات لذلك تجد طرق مختلفة لحماية هذه الشبكات مجال أمن الشبكات مجال واسع ويبقى في مرحلة تطور دائمة ويشمل نطاق دراسته ،. نذكر منها آليات التشفير وإنشاء جدران الحماية أ صل وتاريخ االنترنت ومدى تطورها واألبعاد التي وصلت إليها.