République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Saad Dahleb de Blida

Mémoire de fin d'études

Pour l'obtention du diplôme de master en informatique

Option : Sécurité des Systèmes d'Information

Thème

Contribution à la sécurisation du réseau de la CNEP banque à travers une solution NGFW

Organisme d'accueil : CNEP banque

CNEP Banque

Presidente : Boutaami B.

Réalisé par :

AOUES Meriem Djihen

Koutchouk Aymene

Promotrice :

Dr. Arkam Meriem

Encadrant :

M.Leghmizi Fouzi

Promotion : 2017 / 2018

Remerciements

Nous tenons à remercier en premier lieu ALLAH, le tout puissant, qui nous a donné le courage, la force et la volonté pour bien mener ce modeste travail.

Nos remerciements vont à nos familles, en particulier nos parents pour leurs encouragements.

Nous remercions notre promotrice M.Arkam pour son entière disponibilité.

Nous remercions particulièrement Madame G.Moulahoum pour son accueil chaleureux, et pour la confiance qu'elle nous faite en nous donnons la chance de faire partie de son équipe de sécurité informatique, et de profiter de l'expérience et des compétences du personnel du département Télécommunication et Sécurité Réseau.

Notre reconnaissance va envers notre encadreur Mr F.Leghmizi pour la confiance qu'il nous a accordée en nous proposant ce sujet, également à Mr A.Guiddir qui a énormément contribué à la réalisation de ce travail.

Nous présentons nos gratitudes à notre examinateur qui nous fait l'honneur de juger notre travail.

Finalement, On s'adresse à toute personne ayant contribuée de près ou de loin à la réalisation de ce modeste travail.

Dédicaces

Je dédie ce modeste travail

A mes parents qui n'ont jamais cessé de m'encourager et me soutenir,

A mes deux sœurs,

A ma grande famille,

A mes amis,

A ceux qui me sont chers,

Meriem.

Dédicaces

Je dédie ce modeste travail

A mes parents qui n'ont jamais cessé de m'encourager et me soutenir,

Mon frère,

A mes deux sœurs,

A ma grande famille,

A mes amis,

A ceux qui me sont chers,

Aymene.

Résumé

Face aux diverses menaces, la protection des réseaux des entreprises est plus que jamais à l'ordre du jour. Pour cela, et suite au développement de nouveaux services en ligne, la CNEP banque accorde une attention particulière à la sécurisation de son réseau et tente d'adopter une solide stratégie de protection, C'est dans ce cadre que s'inscrit notre projet.

En effet, l'entreprise manque d'outils nécessaires pour le filtrage du contenu des paquets transitant au travers le réseau pour éliminer les menaces embarquées au contenu tels que les virus, chevaux de Troie, les injections et autres attaques sur les applications web, ou encore pour contrôler les flux applicatifs et gérer la bande passante.
D'autre part, elle est incapable d'analyser le comportement réseau pour détecter les APT[1], les attaques DOS[2], les attaques non répertoriées ou tout autre comportement suspect.

Notre contribution à la sécurisation du réseau de l'entreprise consiste dans un premier temps à mettre en place une nouvelle architecture de sécurité de haute disponibilité en s'appuyant sur l'architecture « DMZ entre deux firewalls » afin de passer à un niveau de sécurité supérieur et garantir la continuité de ses services. Dans un second temps nous adoptons une approche unifiée de gestion de menaces en déployant un NGFW avancé et implémenter ainsi plusieurs technologies de sécurité à la fois, à commencer par de simple règles pare-feu de contrôle d'accès et gestion de bande passante, ensuite nous somme passés à l'analyse de contenu où nous citons : l'analyse antivirale, le contrôle applicatif et le filtrage web. Pour finir avec l'analyse de comportement réseau, il s'agit de : la prévention d'intrusion dynamique, la protection DOS, ainsi que la création d'un réseau virtuel privé.

Mots-clés :

Sécurité réseau, DMZ, firewall, UTM.

---

[1] APT : un type de piratage informatique furtif et continu, nécessite l'utilisation des logiciels malveillants sophistiqués et exige un degré élevé de dissimulation sur une longue période de temps.
[2] DOS : une attaque informatique ayant pour but de rendre indisponible un service.

ملخص :

نظرا للتهديدات المختلفة، أصبحت حماية شبكات الشركات أكثر من أي وقت مضى على جدول الأعمال. لهذا، وبعد تطوير خدمات جديدة على الإنترنت، يولي الصندوق الوطني للتوفير و الاحتياط اهتماما خاصا لأمن شبكته ويحاول تبني استراتيجية قوية للحماية ،و في هذا الإطار يندرج المشروع.

في الواقع ، تفتقر الشركة من الأدوات اللازمة لتصفية محتوى الحزم العابرة عبر الشبكة لإزالة التهديدات المضمنة للمحتوى مثل الفيروسات وأحصنة طروادة والحقن وغيرها من الهجمات على تطبيقات الويب ، أو للتحكم في تدفقات التطبيق وإدارة النطاق الترددي. من ناحية أخرى، يتعذر تحليل سلوك الشبكة للكشف عن APTs أو هجمات DOS أو الهجمات غير المدرجة أو أي سلوك آخر مشبوه.

إن إسهامنا في أمن شبكة الشركة يتكون أولاً من كل شيء في إنشاء بنية أمان جديدة عالية التوفر تعتمد على بنية "DMZ بين جدرتي حماية" للانتقال إلى مستوى الأمان. متفوقة وضمان استمرارية خدماتها. في خطوة ثانية ، نتخذ نهجًا موحدًا لإدارة التهديدات عن طريق نشر NGFW متقدمًا وتطبيق تقنيات أمان متعددة في وقت واحد ، بدءًا من قواعد جدار الحماية للتحكم في الوصول البسيط وإدارة النطاق الترددي ، ذهبنا إلى تحليل المحتوى حيث نقتبس: تحليل مكافحة الفيروسات والتحكم في التطبيقات وتصفية الويب. لإنهاء مع تحليل سلوك الشبكة ، فهو يدور حول: الوقاية من التطفل الديناميكي ، وحماية DOS ، فضلا عن إنشاء شبكة افتراضية.

كلمات البحث:

أمان الشبكة، DMZ، جدار الحماية، UTM

Sommaire

Chapitre 3 : Analyse des besoins

Chapitre 4 : Réalisation, test et validation

Liste des abréviations

APT	Advanced Persistant Threat
ARP	*Address Resolution Protocol*
CLI	Command line Interface
DDOS	Distributed Denial of Service
DLP	Data Leak Prevention
DNS	Domain Name System
DOS	Denial of Service
DPI	Deep Packet Inspection
DTP	Dynamic Threat Prevention
EVE	Emulated Virtual Environnement
FTP	File Transfer Protocol
http	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IDS	Intrusion Detection System
IMAP	Interactive Message Access Protocol
IP	Internet Protocol
IP SEC	Internet Protocol Secure
IPS	Intrusion prevention system
LAN	Local Area Network
NAT	Network Address Translation
NGFW	Next-Generation Firewall
OS	Operating System
OSI	Open Systems Interconnection
POP3	Post Office Protocol
QOS	Quality Of Service
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Socket Layer

UNL	Unified Network Laboratory
URL	Uniform Resource Locator
UTM	Unified Threat Management
VPN	Virtual Private Network
WAF	Web Firewall Application
WAN	Wide Area Network
WUI	Web User Interface
SSI	Sécurité des Systèmes d'Information
CSS	Cross Site Scripting
PPTP	Point-to-Point Tunneling Protocol
L2F	Layer Two Forwarding
L2TP	Layer Two Tunneling Protocol
NIDS	Network Based Intrusion Detection System
HIDS	Host-Based Intrusion Detection System
IDMEF	Intrusion Detection Message Exchange Format
HIPS	Host-based Intrusion Prevention System
WIPS	Wireless Intrusion Prevention System
KIPS	Kernel Intrusion Prevention System
ICSA	International Computer Security Association

Liste des figures

Liste des tableaux

Introduction générale

Depuis l'explosion de la cybercriminalité en 2016, les entreprises ont connu un nombre sans précédent de menaces. Face aux attaques informatiques de plus en plus sophistiquées, la sécurité des entreprises se voit remise en question. Selon une enquête menée par Kaspersky laboratory en 2017, les institutions financières restent les premières visées avec 35%, suivi des portails internet globaux 30.81% et réseaux sociaux 17.32%.

D'autant plus, selon un rapport publié par IBM Security en 2017, 60% des attaques informatiques ayant visées les entreprises en 2016, ont été initiées par quelqu'un de confiance, parfois par malveillance et parfois par inadvertance.

En effet, les attaques informatiques sont lancées par différents types de cybercriminels dont les objectifs sont variés. Quelle que soit leur motivation, ces individus malintentionnés utilisent plusieurs techniques d'attaques : les virus, les chevaux de Troie contenus dans les pièces jointes d'emails, les téléchargements passifs des sites compromis, les injections SQL[1] et autres attaques sur les applications Web ou encore les tactiques d'ingénierie sociale.

Aujourd'hui, un grand nombre de pirates utilisent les attaques persistantes avancées (APT et les attaques mixtes qui combinent plusieurs techniques, et se tournent de plus en plus vers des techniques d'infiltration visant la couche applicative au détriment des attaques réseau qui sont de plus en plus compliquées à mettre en place.

La CNEP banque n'est pas à l'abri. Son système d'information est confronté à des besoins d'évolution grandissants. Il s'agit de la mise à disposition de nouveaux services à ses clients, à l'exemple du e-banking et m-banking permettant le suivi en ligne des comptes bancaires, et bien d'autres services au futur proche. Ceci rend l'ouverture à internet obligatoire et expose l'entreprise aux diverses menaces.

Face aux menaces et aux comportements complice des employés, l'entreprise manque de moyens de protection réseau, d'une part pour détecter et répondre aux menaces embarquées au contenu des paquets, et d'autre part aussi pour détecter et réagir aux comportements suspects et attaques non répertoriées. En plus de l'absence d'outils de gestion des menaces et contrôle de trafic réseau entre les sites de l'entreprise.

[1] Injection SQL : méthodes d'exploitation de faille de sécurité d'une application interagissant avec une base de données.

A cet effet, l'entreprise doit adopter une solide stratégie de protection de ses systèmes informatiques et données bancaires en utilisant différentes technologies de sécurité, pour garantir son rayonnement économique et préserver son image à l'extérieur.

Notre travail consiste dans un premier temps à proposer une architecture réseau plus sécurisée pour l'extranet, en s'appuyant sur une des architectures firewall définies dans la littérature et proposer ainsi quelques améliorations. Dans un second temps, il s'agit de déployer une nouvelle génération de firewalls permettant de mettre en place plusieurs technologies de sécurité toutes ensemble, dans le but de fournir un niveau de sécurité le plus élevé possible.

Afin de présenter notre travail, le mémoire est réparti en quatre chapitres et s'organise comme suit :

- Un premier chapitre comprenant l'état de l'art. Il souligne les aspects théoriques du domaine de la sécurité informatique, en évoquant les définitions et concepts de base, ainsi que les moyens usuels de protection réseau.

- Un deuxième chapitre qui s'intéresse quant à lui aux notions relatives aux firewalls et leur évolution, et montre ainsi leur importance dans l'entreprise vue leur capacité à fournir un niveau de sécurité élevé.

- Le troisième chapitre consiste d'abord à prendre connaissance du réseau informatique de l'entreprise d'accueil, ensuite nous expliquons ses vulnérabilités, puis nous proposons une solution pour d'une part combler les faiblesses existantes, d'autre part renforcer la sécurité du système d'information et assurer les performances des communications réseau. pour accompagner son développement, à savoir la proposition d'une architecture de sécurité pour l'extranet et le déploiement.

- Nous proposons dans le quatrième chapitre une simulation de notre solution, ou nous présentons d'abord les outils utilisés. Ensuite, nous expliquons les différentes étapes de réalisation de la solution, pour terminer avec quelques tests et résultats afin de valider notre démarche.

- Nous terminons par une conclusion mettant en évidence notre travail et quelques perspectives.

Chapitre I : Sécurité informatique

1. Introduction :

L'utilisation extensive d'internet a incitée les entreprises d'ouvrir leurs systèmes d'information à leurs partenaires ou leurs fournisseurs. Tout ordinateur connecté à Internet et d'une manière plus générale à n'importe quel réseau informatique, est susceptible d'être victime d'une attaque informatique. Il est donc nécessaire de se protéger de ces attaques réseaux en mettant en place un ensemble des moyens de protection selon les ressources à protéger.

L'objet de ce chapitre est de donner un bref aperçu sur la sécurité des systèmes d'information, en particulier la sécurité réseau. Nous commençons par présenter quelques notions introductives, ensuite nous détaillerons les différents moyens et dispositifs de protection des réseaux informatiques.

2. Sécurité des systèmes d'information :

Dans cette section nous donnons un bref aperçu sur les notions de base de la sécurité des systèmes d'information, et son champ d'application dans les entreprises.

2.1 Définition :

La sécurité des systèmes d'information (SSI) ou plus simplement sécurité informatique, est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires à la mise en place de moyens visant à empêcher l'utilisation non-autorisée, le mauvais usage, la modification ou le détournement du système d'information. Assurer la sécurité du système d'information est une activité du management du système d'information, (Ouahrani, 2015).

2.2 Objectifs de sécurité :

Le système d'information représente un patrimoine essentiel de l'organisation, qu'il convient de protéger. La sécurité informatique consiste à garantir que les ressources matérielles ou logicielles

d'une organisation sont uniquement utilisées dans le cadre prévu. La sécurité des systèmes d'information vise les objectifs suivants :

- La disponibilité : le système doit fonctionner sans faille durant les plages d'utilisation prévues et garantir l'accès aux services et ressources installées avec le temps de réponse attendu.
- L'intégrité : les données doivent être celles que l'on attend, et ne doivent pas être altérées de façon fortuite, illicite ou malveillante. En clair, les éléments considérés doivent être exacts et complets.
- La confidentialité : seules les personnes autorisées peuvent avoir accès aux informations qui leur sont destinées. Tout accès indésirable doit être empêché.

D'autres aspects peuvent aussi être considérés comme des objectifs de la sécurité des systèmes d'information, tels que :

- La traçabilité (ou « preuve ») : garantie que les accès et tentatives d'accès aux éléments considérés sont tracés et que ces traces sont conservées et exploitables.
- L'authentification: l'identification des utilisateurs est fondamentale pour gérer les accès aux espaces de travail pertinents et maintenir la confiance dans les relations d'échange.
- La non-répudiation et l'imputation : aucun utilisateur ne doit pouvoir contester les opérations qu'il a réalisées dans le cadre de ses actions autorisées et aucun tiers ne doit pouvoir s'attribuer les actions d'un autre utilisateur.

Une fois les objectifs de la sécurisation déterminés, les risques pesant sur chacun de ces éléments peuvent être estimés en fonction des menaces. Le niveau global de sécurité des systèmes d'information est défini par le niveau de sécurité du maillon le plus faible. Les précautions et contre-mesures doivent être envisagées en fonction des vulnérabilités propres au contexte auquel le système d'information est censé apporter service et appui.

2.3 Champs d'application de la SSI :

Pour une organisation, toutes les sphères d'activité de l'informatique et des réseaux de télécommunication sont concernées par la sécurité d'un système d'information. En fonction de son domaine d'application, la sécurité informatique se décline en :

- sécurité physique et environnementale.
- sécurité de l'exploitation.
- sécurité logique.
- sécurité applicative et sécurité de l'information.
- sécurité des infrastructures informatique et de télécommunication (sécurité des réseaux, sécurité Internet et cybersécurité).

3. Sécurité réseau :

3.1 Définition :

La sécurité d'un réseau est un niveau de garantie que l'ensemble des machines du réseau fonctionnent de façon optimale et que les utilisateurs desdites machines possèdent uniquement les droits qui leur ont été octroyés. En résumé, elle consiste à offrir une connectivité de bout en bout, qu'elle soit sécurisée et de qualité, (Baouya, 2018).

3.2 Moyens de protection réseau :

Pour avoir un réseau sécurisé et complémentaire, les entreprises intègrent plusieurs moyens de sécurité pour que l'un couvre les lacunes de l'autre, et ce dont le but de protéger les attaques réseau. Cette section est consacrée à l'étude des moyens de protection réseau usuels.

3.2.1 Serveur mandataire (Proxy) :

a. Présentation :

Un serveur Proxy, appelé aussi serveur mandataire est à l'origine une machine faisant fonction d'intermédiaire entre les ordinateurs d'un réseau local, utilisant parfois des protocoles autre que le protocole TCP/IP et Internet.

La plupart du temps le serveur Proxy est utilisé pour le web, il s'agit alors d'un Proxy HTTP. Toutefois, il peut exister des serveurs Proxy pour chaque protocole applicatif (FTP, etc.).

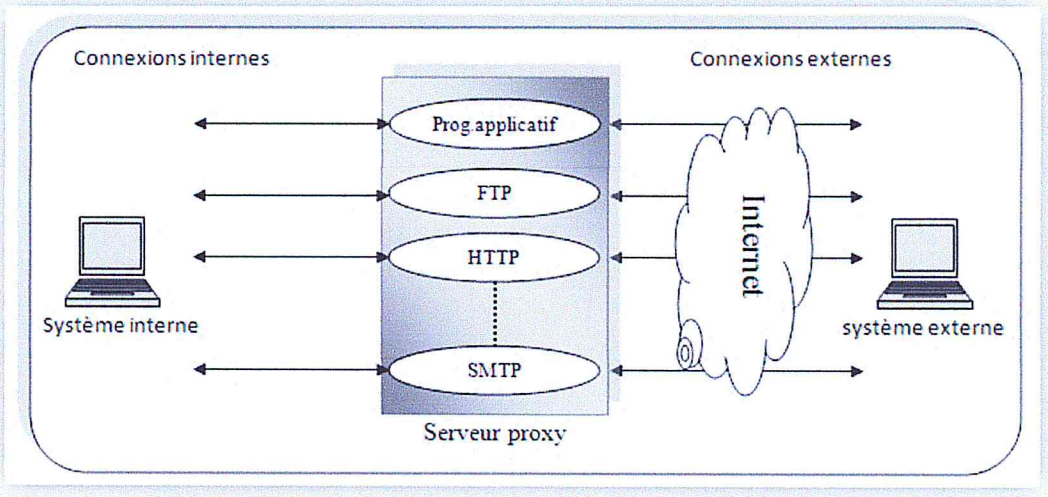


Figure 1.6 : Architecture d'un proxy

b. Principe de fonctionnement :

Le principe de fonctionnement d'un serveur Proxy est assez simple : il établit un lieu et place de l'utilisateur et le service invoqué par celui-ci (FTP, etc.) (Figure 1.6). Ainsi lorsqu'un utilisateur se connecte à l'aide d'une application cliente configurée pour utiliser un serveur Proxy, celle-ci va se connecter en premier lieu au serveur proxy et lui donner sa requête. Le serveur Proxy va alors se connecter au serveur que l'application cliente cherche à joindre et lui transmettre la requête (le serveur Proxy contacte le serveur externe sollicité sur internet avec sa propre adresse ou une adresse issue d'un pool d'adresses IP libres). Le serveur va ensuite donner sa réponse au Proxy, qui va à son tour la transmettre à l'application cliente. Le Proxy cache de la sorte toute l'infrastructure du réseau local et ne dévoile en aucun cas les adresses des machines internes (masquage d'adresse), (Ghernaouti, 2013).

c. Fonctionnalité d'un serveur proxy :

Avec l'utilisation de TCP/IP au sein des réseaux locaux, le rôle de relais du serveur proxy est directement assuré par les passerelles et les routeurs. Les serveurs Proxys sont toujours d'actualité grâce à un certain nombre d'autres fonctionnalités.

- **Cache :**

La plupart des Proxys assurent ainsi une fonction de cache (caching), c'est-à-dire la capacité à garder en mémoire (en « cache ») les pages les plus souvent visitées par les utilisateurs du réseau local afin de pouvoir les leur fournir le plus rapidement possible. En effet, en informatique, le

terme de « cache » désigne un espace de stockage temporaire de données (le terme de « tampon » est également parfois utilisé).

Un serveur Proxy ayant la possibilité de cacher (néologisme signifiant « mettre en mémoire cache ») les informations est généralement appelé serveur Proxy-cache.

Cette fonctionnalité implémentée dans certains serveurs Proxy permet d'une part de réduire l'utilisation de la bande passante vers Internet ainsi que de réduire le temps d'accès aux documents pour les utilisateurs.

Toutefois, pour mener à bien cette mission, il est nécessaire que le Proxy compare régulièrement les données qu'il stocke en mémoire cache avec les données distantes afin de s'assurer que les données en cache sont toujours valides.

- **Filtrage :**

D'autre part, grâce à l'utilisation d'un Proxy, il est possible d'assurer un suivi des connections via la constitution des journaux d'activités (logs) en enregistrant systématiquement les requêtes des utilisateurs lors de leurs demandes de connexion à Internet.

Il est ainsi possible de filtrer les connexions à internet en analysant d'une part les requêtes des clients, d'autre part les réponses des serveurs.

Le filtrage basé sur l'adresse des ressources consultées est appelé filtrage d'URL.

Lorsque le filtrage est réalisé en comparant la requête du client à une liste de requêtes autorisées, on parle de liste blanche ; lorsqu'il s'agit d'une liste de sites interdits, on parle de liste noire.

En fin l'analyse des réponses des serveurs conformément à une liste de critères (mots- clés….) est appelée filtrage de contenu.

- **Authentification :**

Dans la mesure où le Proxy est l'intermédiaire indispensable des utilisateurs du réseau interne pour accéder à des ressources externes, il est parfois possible de l'utiliser pour authentifier les utilisateurs, c'est–à-dire de leur demander de s'identifier à l'aide d'un nom d'utilisateur et d'un mot de passe par exemple. Il est ainsi aisé de donner l'accès aux ressources externes aux seules personnes autorisées à le faire et de pouvoir enregistrer dans les fichiers journaux des accès identifiés. Ce type de mécanisme, lorsqu'il est mise en œuvre, pose bien évidement de nombreux problèmes relatifs aux libertés individuelles et aux droits des personnes.

3.2.2 Translation Adresses(NAT) :

Son principe consiste à modifier l'adresse IP source ou destination, dans l'en-tête d'un datagramme IP lorsque le paquet transite dans le Pare-feu (Proxy) en fonction de l'adresse source ou destination et du port source ou destination.

Lors de cette opération, le Pare-feu garde en mémoire l'information lui permettant d'appliquer la transformation inverse sur le paquet de retour. La traduction d'adresse permet de masquer le plan d'adressage interne (non routable) à l'entreprise par une ou plusieurs adresses routables sur le réseau externe ou sur Internet. Cette technologie permet donc de cacher le schéma d'adressage réseau présent dans une entreprise derrière un environnement protégé, (Ghernaouti, 2013).

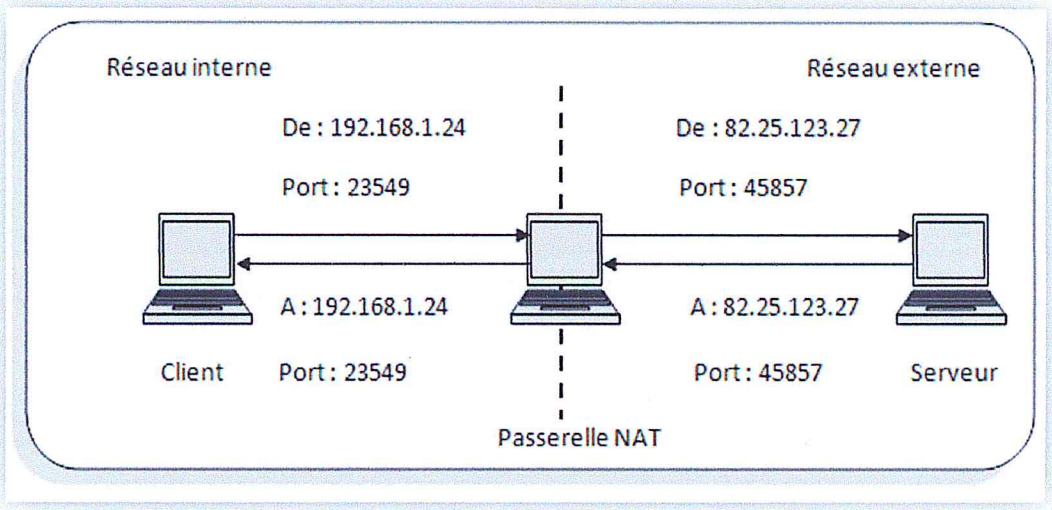


Figure 1.7 : Mécanisme de translation d'adresses

a. Translation Statique :

Le principe du NAT statique consiste à associer une adresse IP publique à une adresse IP privée interne au réseau. La passerelle permet donc d'associer à une adresse IP privée (Par exemple 192.168.0.1) une adresse IP publique routable sur Internet et de faire la traduction, dans un sens comme dans l'autre, en modifiant l'adresse dans le paquet IP.

La translation d'adresse statique permet ainsi de connecter des machines du réseau interne à Internet de manière transparente mais ne résout pas le problème de la pénurie d'adresse dans la mesure où n adresses IP routables sont nécessaires pour connecter n machines du réseau interne.

b. Translation Dynamique :

Le NAT dynamique permet de partager une adresse IP routable (ou un nombre réduit d'adresses IP routables) entre plusieurs machines en adressage privé. Ainsi, toutes les machines du réseau interne possèdent virtuellement, vu de l'extérieur, la même adresse IP.

Afin de pouvoir « multiplexer » (partager) les différentes adresses IP sur une ou plusieurs adresses IP routables, le NAT dynamique utilise le mécanisme de translation de port (PAT, Port Address Translation), c'est-à-dire l'affectation d'un port source différent à chaque requête de telle manière à pouvoir maintenir une correspondance entre les requêtes provenant du réseau interne et les réponses des machines sur Internet, toutes adressées à l'adresse IP de la passerelle.

3.2.3 Réseaux Privé virtuels :

a. Présentation :

Il arrive ainsi souvent que les entreprises éprouvent le besoin de communiquer avec les filiales, des clients ou même du personnel géographiquement éloigné via internet.

Pour autant, les données transmises sur Internet sont beaucoup plus vulnérables que lorsqu'elles circulent sur un réseau interne à une organisation car le chemin emprunté n'est pas défini à l'avance, ce qui signifie que les données empruntent une infrastructure réseau publique appartenant à différents opérateurs. Ainsi, il n'est pas impossible que sur le chemin parcouru, le réseau soit écouté par un utilisateur indiscret ou même détourné. Il n'est donc pas concevable de transmettre dans de telles conditions des informations sensibles pour l'organisation ou l'entreprise.

La solution consiste à utiliser Internet comme support de transmission en utilisant un protocole d'encapsulation (tunneling), c'est-à-dire encapsulant les données à transmettre de façon chiffrée. On parle alors de réseau privé virtuel (noté RPV ou VPN, Virtual Private Network) pour désigner le réseau ainsi artificiellement créé.

Ce réseau est dit virtuel car il relie deux réseaux « physiques » (réseaux locaux) par une liaison non fiable (Internet), et privé car seuls les ordinateurs des réseaux locaux de part et d'autre du VPN peuvent voir les données, (Ghernaouti, 2013).

b. Mise en œuvre de liaisons sécurisées :

L'échange de données confidentielles entre les personnels nomades et l'entreprise ou entre différentes entités implique la mise en œuvre de liaisons sécurisées, physiques (lignes louées spécialisées) ou virtuelles (VPN) en liaison avec un Pare-feu.

L'échange de données entre sites distants de la même entreprise peut aussi être effectué en utilisant une liaison spécialisée ou dédiée utilisant les services d'un opérateur de télécommunication. Cette solution permet de s'affranchir de toutes les menaces liées à l'utilisation du réseau Internet, mais elle représente un coût plus important.

c. Fonctionnement d'un VPN :

Un réseau privé virtuel repose sur un protocole, appelé protocole de tunneling, c'est- à-dire un protocole permettant aux données passant d'une extrémité du VPN à l'autre d'être sécurisées par des algorithmes de cryptographie.

L'expression tunnel chiffré est utilisée pour symboliser le fait qu'entre l'entrée et la sortie du VPN, les données sont chiffrées (cryptées) et donc incompréhensibles pour toute personne située entre les deux extrémités du VPN, comme si les données passaient dans un tunnel. Dans le cas d'un VPN établi entre deux machines, on appelle client VPN, l'élément permettant de chiffrer et de déchiffrer les données du côté utilisateur (client) et serveur VPN (ou plus généralement serveur d'accès distant) l'élément chiffrant et déchiffrant les données du côté de l'organisation.

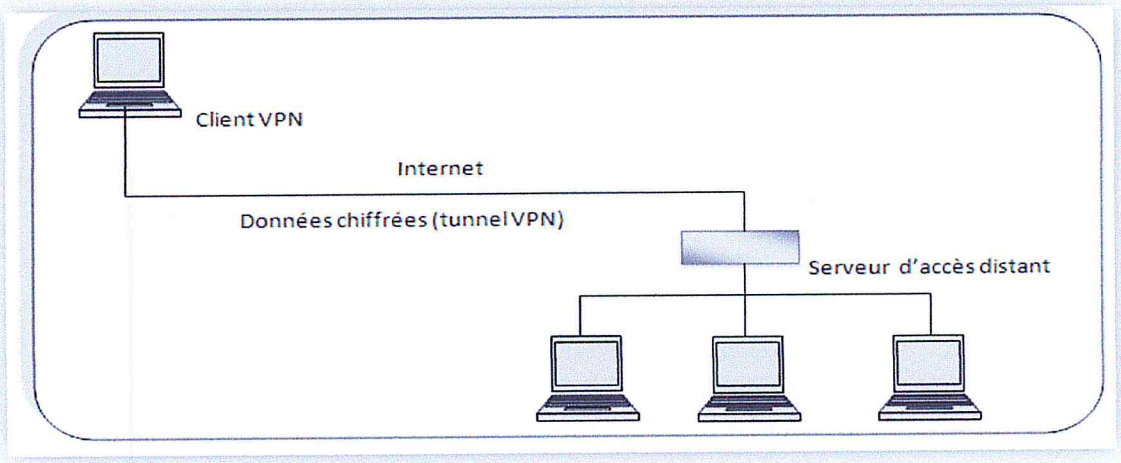


Figure 1.9 Réseau Privé Virtuel (VPN)

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

L'ordinateur distant va alors fournir les données au serveur VPN de son réseau local qui va transmettre la réponse de façon chiffrée. A la réception sur le client VPN de l'utilisateur, les données seront déchiffrées, puis transmises à l'utilisateur.

d. Protocoles de tunneling :

Les principaux protocoles de tunneling sont les suivants :

- **PPTP** (point-to-point tunneling protocol) est un protocole de niveau 2 développé par Microsoft en collaboration avec d'autres entreprises.
- **L2F** (Layer Two Forwarding) est un protocole de niveau 2 développé par Cisco. Il est désormais quasi obsolète.
- **L2TP** (Layer Two Tunneling Protocol) Il s'agit ainsi d'un protocole de niveau 2.
- **IPSec** est un protocole de niveau 3, permettant de transporter des données chiffrées pour les réseaux IP.

3.2.4 Zone démilitarisée :

Les systèmes pare-feu permettent de définir des règles d'accès entre deux réseaux. Néanmoins, dans la pratique, les entreprises ont généralement plusieurs sous-réseaux avec des politiques de sécurité différentes. C'est la raison pour laquelle il est nécessaire de mettre en place des architectures de systèmes pare-feu permettant d'isoler les différents réseaux de l'entreprise : on parle ainsi de « cloisonnement des réseaux » (le terme isolation est parfois également utilisé).

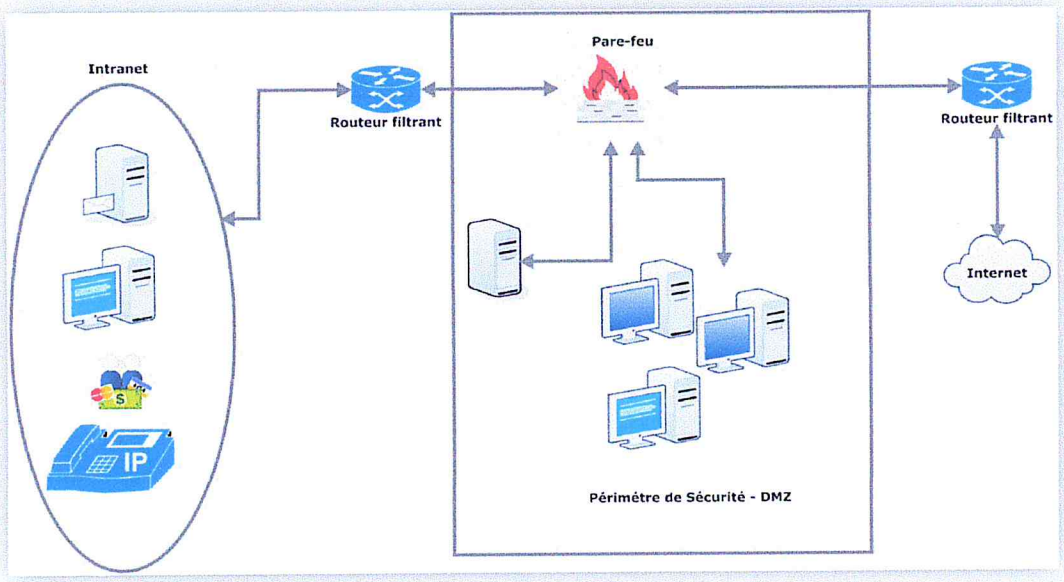


Figure 1.10 Architecture DMZ

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

disposition du public. La DMZ fait ainsi office de « zone tampon » entre le réseau à protéger et le réseau hostile. La figure ci-dessous montre la position d'une DMZ au sein d'un réseau, les serveurs situés dans la DMZ sont appelés « bastions » en raison de leur position d'avant-poste dans le réseau de l'entreprise, (Ghernaouti, 2013). la politique de sécurité mise en œuvre sur la DMZ est généralement la suivante :

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

La DMZ possède donc un niveau de sécurité intermédiaire, mais son niveau de sécurisation n'est pas suffisant pour y stocker des données critiques pour l'entreprise. Il est à noter qu'il est possible de mettre en place des DMZ en interne afin de cloisonner le réseau interne selon différents niveaux de protection et ainsi éviter les intrusions venant de l'intérieur.

3.2.5 Système de détection d'intrusion :

Un système de détection d'intrusion est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte). Il permet ainsi d'avoir une connaissance sur les tentatives réussies comme échouées des intrusions.

a. Les familles de systèmes de détection d'intrusion :

Il existe trois grandes familles de systèmes de détection d'intrusion :

i. IDS Réseau :

Un IDS se découpe en trois grandes parties :

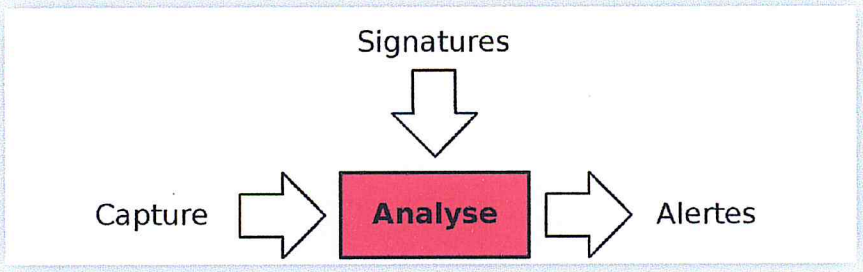


Figure 1.11 Schéma simplifié d'un NIDS

- **Capture :**

La capture sert à la récupération de trafic réseau. En général cela se fait en temps réel, bien que certains NIDS permettent l'analyse de trafic capturé précédemment, La plupart des NIDS utilisent la bibliothèque standard de capture de paquets libpcap[2]. La bibliothèque de capture de paquets est portée sur quasiment toutes les plates-formes.

- **Signature :**

Les bibliothèques de signatures (approche par scénario) rendent la démarche d'analyse similaire à celle de l'antivirus quand ceux-ci s'appuient sur des signatures d'attaques. Ainsi, le NIDS est efficace s'il connaît l'attaque, mais inefficace dans le cas contraire. Les outils commerciaux ou libres ont évolué pour proposer une personnalisation de la signature afin de faire face à des attaques dont on ne connaît qu'une partie des éléments. Les outils à base de signatures requièrent des mises à jour très régulières. Les NIDS ont pour avantage d'être des systèmes temps réel et ont la possibilité de découvrir des attaques ciblant plusieurs machines à la fois. Leurs inconvénients sont le taux élevé de faux positifs qu'ils génèrent, le fait que les signatures aient toujours du retard sur les attaques de type zéro day et qu'ils puissent être la cible d'une attaque.

- **Alerte :**

Les alertes sont généralement stockées dans les journaux du système. Cependant, il existe une norme qui permet d'en formaliser le contenu, afin de permettre à différents éléments de sécurité d'inter-opérer. Ce format s'appelle IDMEF (Intrusion Detection Message Exchange Format) est popularisé par le projet Prelude, qui offre une infrastructure permettant aux IDS de ne pas avoir à s'occuper de l'envoi des alertes. Cela permet aux IDS de n'avoir qu'à décrire les informations qu'ils connaissent et Prelude se charge de les stocker pour permettre une visualisation humaine ultérieure.

ii. IDS hôte :

Les HIDS, pour Host based IDS, signifiant "Système de détection d'intrusion machine" sont des IDS dédiés à un matériel ou système d'exploitation. Généralement, et contrairement à un NIDS, le HIDS récupère les informations qui lui sont données par le matériel ou le système d'exploitation. Il y a pour cela plusieurs approches : signatures, comportement (statistiques)

[2] libpcap: est une interface de programmation permettant de capturer un trafic réseau.

ou délimitation du périmètre avec un système d'ACL. Un HIDS se comporte comme un daemon ou un service standard sur un système hôte qui détecte une activité suspecte en s'appuyant sur une norme. Si les activités s'éloignent de la norme, une alerte est générée. La machine peut être surveillée sur plusieurs points :

- Activité de la machine : nombre et listes de processus ainsi que d'utilisateurs, ressources consommées, ...
- Activité de l'utilisateur : horaires et durée des connexions, commandes utilisées, messages envoyés, programmes activés, dépassement du périmètre défini...
- Activité malicieuse d'un ver, virus ou cheval de Troie

Un autre type d'HIDS cherche les intrusions dans le « noyau »du système, et les modifications qui y sont apportées. Certains appellent cette technique « analyse protocolaire ». Très rapide, elle ne nécessite pas de recherche dans une base de signature.

Le HIDS a pour avantage de n'avoir que peu de faux positifs, permettant d'avoir des alertes pertinentes. Quant à ses inconvénients il faut configurer un HIDS par poste et il demande une configuration de chaque système.

iii. IDS hybride :

Les IDS hybrides sont basés sur une architecture distribuée, où chaque composant unifie son format d'envoi d'alerte (typiquement IDMEF) permettant à des composants divers de communiquer et d'extraire des alertes plus pertinentes.

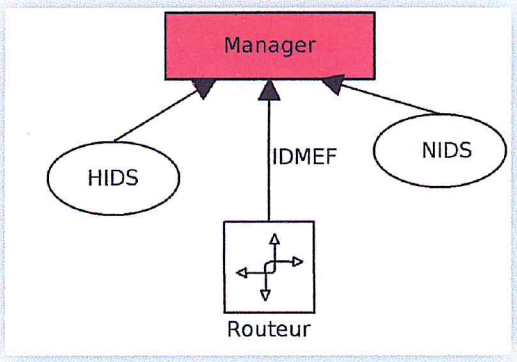


Figure 1.12 schéma simplifié d'un IDS hybride

Les avantages des IDS hybrides sont multiples :

- Moins de faux positifs
- Meilleure corrélation
- Possibilité de réaction sur les analyseurs

3.2.6 Systeme de prevention d'intrusion (IPS):

a. Présentation :

Un système de prévention d'intrusion est un outil des spécialistes en sécurité des systèmes d'information, similaire aux IDS, permettant de prendre des mesures afin de diminuer les impacts d'une attaque. C'est un IDS actif, il détecte un balayage automatisé, l'IPS peut bloquer les ports automatiquement. Les IPS peuvent donc parer les attaques connues et inconnues. Comme les IDS, ils ne sont pas fiables à 100 % et risquent même en cas de faux positif de bloquer du trafic légitime.

b. Types de système de prévetion d'intrusion :

Il existe trois types de systèmes de prévention d'intrusion :

- Les HIPS (host-based intrusion prevention system) qui sont des IPS permettant de surveiller le poste de travail à travers différentes techniques, ils surveillent les processus, les drivers, les .dll etc. En cas de détection de processus suspect le HIPS peut le tuer pour mettre fin à ses agissements. Les HIPS peuvent donc protéger des attaques de buffer overflow.
- Les NIPS (network intrusion prevention system) sont des IPS permettant de surveiller le trafic réseau, ils peuvent prendre des mesures telles que terminer une session TCP. Une déclinaison en WIPS (wireless intrusion prevention system) est parfois utilisée pour évoquer la protection des réseaux sans-fil.
- Il existe aussi les KIPS (kernel intrusion prevention system) qui permettent de détecter toutes tentatives d'intrusion au niveau du noyau, mais ils sont moins utilisés.

Les IPS ne sont pas des logiciels miracle qui vous permettront de surfer en toute quiétude sur le net. Voici quelques-uns de leurs inconvénients :

- Ils bloquent tout ce qui parait infectieux à leurs yeux, mais n'étant pas fiable à 100 % ils peuvent donc bloquer malencontreusement des applications ou des trafics légitimes.

- Ils laissent parfois passer certaines attaques sans les repérer.
- Ils sont peu discrets et peuvent être découverts lors de l'attaque d'un pirate qui une fois qu'il aura découvert l'IPS s'empressera de trouver une faille dans ce dernier pour le détourner et arriver à son but.

4. Conclusion :

Nous avons commencés le présent chapitre par quelques notions de base du domaine de la sécurité des systèmes d'information, pus nous nous sommes tournés vers la sécurité réseau pour approfondir dans les moyens de protection réseau les plus utilisés. Malgré le niveau de sécurité qu'ils peuvent apportés, le firewall reste le moyen le plus répandu et la solution la plus complète surtout après les dernières évolutions qu'il a connu.

Pour cela, nous consacrons le chapitre suivant à l'étude des concepts fondamentaux, inhérents aux firewalls, nous l'entamons par des définitions de base, puis nous expliquons son principe de fonctionnement, ensuite nous présentons les différentes architectures firewalls existantes. Enfin, nous nous intéressons à leur évolution pour comprendre le passage d'un firewall classique à un NGFW avancé.

Chapitre II: Généralités sur les firewalls

1. Introduction :

Les firewalls sont des éléments très important pour la sécurité du réseau de toute entreprise, ils ont connu une évolution au fil du temps dans le foyer de l'industrie pour pouvoir faire face aux nouveaux enjeux. Cette évolution va de pair avec l'évolution considérable des attaques contre les réseaux, le ressources et les utilisateurs des entreprises, ainsi que l'apparition de nouvelles techniques et outils d'attaques, pour contourner les mesures de sécurité traditionnelles, ainsi que l'évolution des applications et services proposées par les entreprises.

L'objet de ce chapitre est de définir les concepts inhérents aux firewalls et montrer leurs évolution, nous allons l'entamer par la définition d'un firewall et la description de son principe de fonctionnement, nous présentons par la suite les différentes architectures firewalls existantes, suivi par les fonctionnalités intégrées au sein des firewalls classiques, ainsi notre une étude portera sur les pare-feu de nouvelle génération, enfin nous montrons les dernières évolutions des firewalls en terme de fonctionnalités de protection .

2. Firewalls classiques :

2.1 Définition et principe :

Le firewall est un système qui sert d'interface entre un ou plusieurs réseaux. C'est un dispositif technique qui appuie la politique et les besoins d'une entreprise en matière de sécurité par le moyen de services de contrôle d'accès, d'authentification et de vérification. Plus concrètement, c'est un outil qui agit comme barrière qui contrôle le passage des flux d'information entre le réseau interne de l'entreprise et un réseau public (internet ou autre). Ce dernier bloque éventuellement certaines données et neutralise les tentatives de pénétration en provenance du réseau public, (Chaouchi, 2015).

En effet, un système firewall contient un ensemble de règles prédéfinies permettant de mettre en œuvre une méthode de filtrage dépendant de la politique de sécurité adoptée par l'entreprise.

On distingue deux types de politiques de sécurité :

- Soit autoriser uniquement les communications ayant été explicitement autorisées.
- Soit empêcher les échanges qui ont été explicitement interdits.

Le firewall est en général installé sur une machine séparée du reste de réseau de façon à ce qu'une requête entrante ne puisse directement atteindre les ressources locales.

2.2 Types de filtrage :

Il existe trois principaux types de filtrage, regroupés comme suit :

2.2.1 Filtrage sans état (stateless) :

Cette méthode est considérée comme la plus simple, elle est effectuée au niveau de la couche réseau et de la couche transport. En effet, ce type de filtrage consiste à regarder chaque paquet indépendamment des autres et le compare à une liste de règles.

Il permet d'accepter ou de refuser le passage de paquet d'un réseau à un autre en fonction de l'adresse IP source et celle de destination, et le numéro de port source et celui de destination et le protocole de couche réseau ou transport.

Bien que le filtrage simple de paquet soit performant, l'élaboration des règles est assez difficile. De même, il ne permet pas d'analyser le contenu des paquets reçus. L'acceptation ou le refus d'un paquet étant uniquement basée sur son enveloppe et son état, il sera donc impossible de faire du filtrage antivirus, (Chaouchi, 2015).

2.2.2 Filtrage à état (statefull) :

L'amélioration par rapport au filtrage sans état réside dans sa capacité à conserver la trace des sessions et des connexions dans des tables d'états internes au firewall. En effet, ce filtrage est capable d'évaluer un paquet dans le contexte de la connexion à laquelle il appartient grâce à ces tables d'états et peut rapidement déterminer si un paquet fait partie d'une connexion déjà établie et autorisée. Si c'est le cas, le paquet est transféré sans test complémentaire.

La conservation de l'état des connexions a pur avantage de simplifier les règles de filtrage et d'améliorer les performances. Ce filtrage permet ainsi de se protéger à certains types d'attaques Déni de service. Toutefois, il ne se protège pas contre les failles applicatives liées aux logiciels, qui représentent les risques les plus importants en matière de sécurité. (Chaouchi, 2015).

2.2.3 Filtrage applicatif :

Le filtrage applicatif est réalisé au niveau de la couche application, il permet d'extraire les données du protocole de niveau 7 pour les analyser. Les requêtes sont traitées par des processus dédiées. Par exemple, une requête de type http sera filtrée par un proxy http, toutes les requêtes qui ne sont pas conformes aux spécifications du protocole seront rejetées.

Les firewalls effectuant du filtrage applicatif est appelé passerelle applicative du fait qu'il permet de relayer des informations entre deux réseaux en effectuant un filtrage fin au niveau des paquets échangés. Il s'agit d'un dispositif performant assurant une bonne protection du réseau, (Chaouchi, 2015).

Avec ce type de filtrage les politiques de sécurité sont plus flexibles et efficaces puisque toutes les informations contenues dans les paquets peuvent être utilisées pour écrire les règles servant à déterminer les paquets bloqués par le filtre. En contrepartie, une analyse fine des données applicatives requiert une grande puissance de calcul et se traduit par un ralentissement des communications.

3. Architectures firewall :

Il existe différents types de technologies firewall, communément appelées architectures firewall, dans ce qui suit nous présenterons les architectures firewall ainsi que les variantes possibles.

3.1 Architecture avec routeur de filtrage :

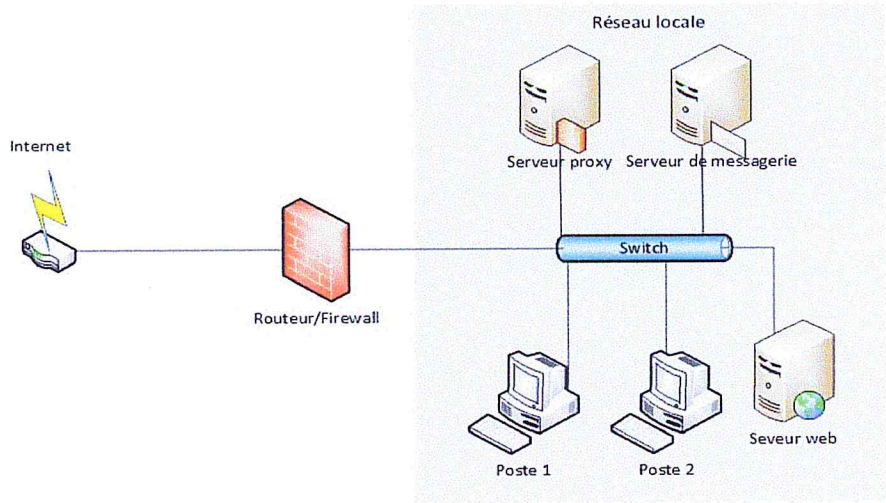


Figure 2.1 : Firewall avec routeur de filtrage

La figure 2.1 illustre l'architecture firewall avec routeur de filtrage, c'est la solution firewall la plus simple, elle consiste à interconnecter un réseau privé à l'internet par l'intermédiaire d'un routeur de filtrage. Celui-ci contient les autorisations d'accès basées sur les adresses IP et les numéros de port qui représentent les numéros d'identification de chacun des ordinateurs.

3.2 Architecture réseau bastion :

On appelle une machine bastion tout firewall de niveau application conçu pour protéger et résister au maximum contre certaines vulnérabilités. Elle fonctionne au niveau applicatif contrairement au routeur filtrant qui fonctionne au niveau réseau.

On peut identifier deux sortes d'architecture avec machine bastion à savoir Single-Homed firewalls et Dual-Homed firewalls.

3.2.1 Single-Homed bastion host :

Ce type de firewall, présenté par **la figure 2.2**, utilise à la fois une machine bastion et un routeur de filtrage de paquets.

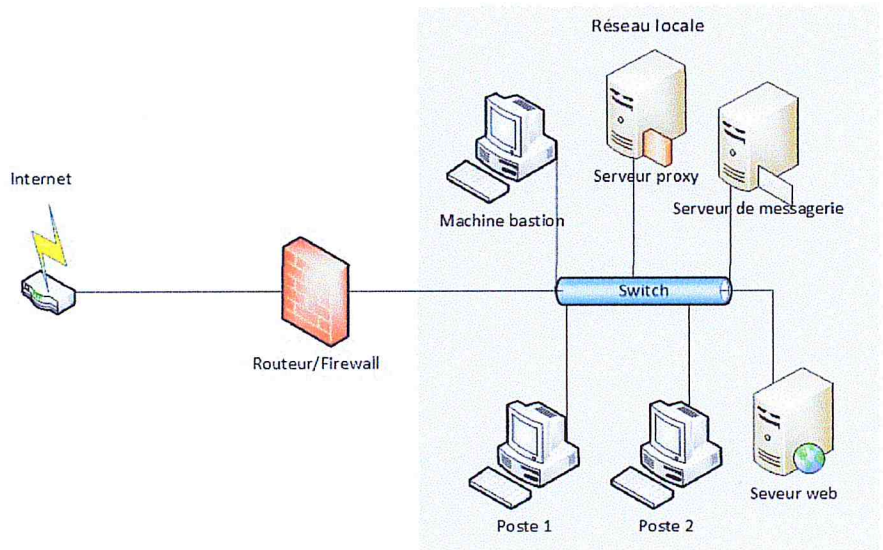


Figure 2.2: Single-Homed bastion host

Après avoir effectué un premier tri des paquets provenant de l'extérieur à l'aide de filtres, le routeur les envoie à la machine bastion en modifiant l'adresse IP de destination et en rajoutant au paquet l'adresse initiale de destination. Après traitement, la machine bastion renvoie ce paquet à l'adresse adéquate.

Comme les hôtes internes se trouvent sur le même réseau que la machine bastion, ce sont les règles de sécurité de l'entreprise qui déterminent dans quels cas une communication doit passer vers l'extérieur et dans quels cas elle doit être bloquée.

Bien que le bastion constitue une protection efficace, une fois que les intrusions malveillantes ont droits d'accès, ils se propagent à l'intérieur de la totalité du réseau.

C'est pourquoi ce type de protection est considéré comme non sécuritaire.

3.2.2 Dual-Homed bastion host :

Cette solution permet de remédier au problème posé par le Single-Homed bastion host. Dans ce système, la machine bastion possède deux interfaces reliant le réseau privé au routeur de filtrage de paquets.

Le principal avantage de ce système est qu'il n y a pas de liaison directe entre le réseau public et privé ce qui augmente le niveau de sécurité. La machine bastion est la seule machine visible depuis internet, il suffit d'interdire les utilisateurs internes de se connecter à la machine bastion pour éviter les failles de sécurité.

La figure 2.3 illustre cette solution :

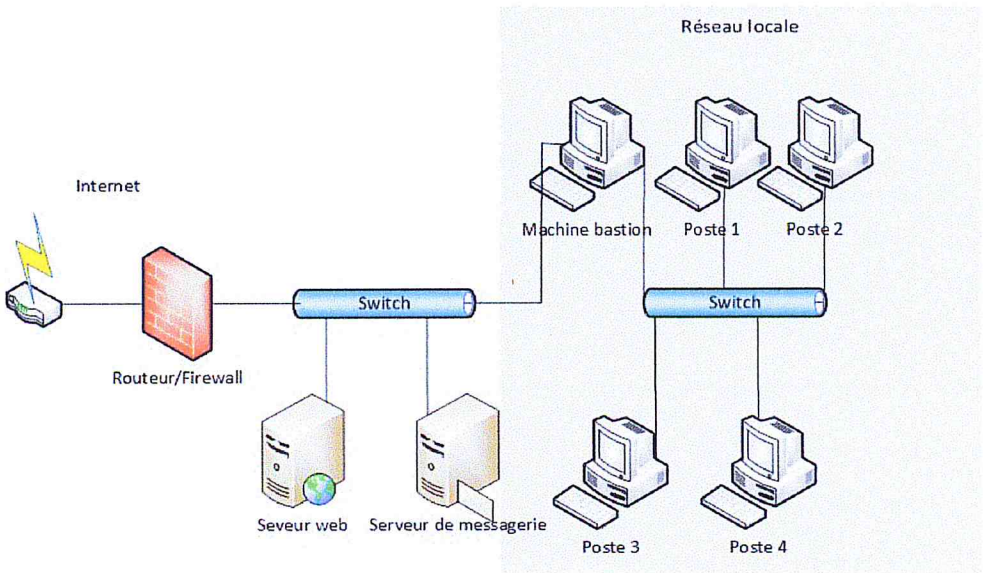


Figure 2.3 : Dual-Homed bastion host

3.3 Architecture avec zone démilitarisée :

En pratique, les entreprises ont généralement plusieurs sous-réseaux avec des politiques de sécurité différentes, C'est la raison pour laquelle il est nécessaire de mettre en place des

architectures permettant d'isoler les différents réseaux de l'entreprise : on parle ainsi de « cloisonnement réseau ».

Lorsque certaines machines du réseau interne ont besoin d'être accessibles de l'extérieur, elles sont souvent isolées dans un sous réseau à part entière connu par « zone démilitarisé ».

Il existe deux sortes d'architecture avec DMZ, à savoir DMZ entre deux firewalls et Firewall à trois interfaces.

3.3.1 DMZ entre deux firewalls :

Ce système utilise deux firewalls afin de créer un sous réseau filtré. En effet, le sous réseau filtré désigne la zone démilitarisée qui s'intercale entre le réseau public et le réseau local. Les serveurs publics (WEB, MAIL, DNS,…) sont placés à l'intérieur avec le bastion host. Ils ne résident pas dans le réseau local, la DMZ est configurée pour que les systèmes internes et externes ne puissent accéder qu'à des limites services, sachant que le trafic direct à travers la DMZ est interdit, (Chaouchi, 2015).

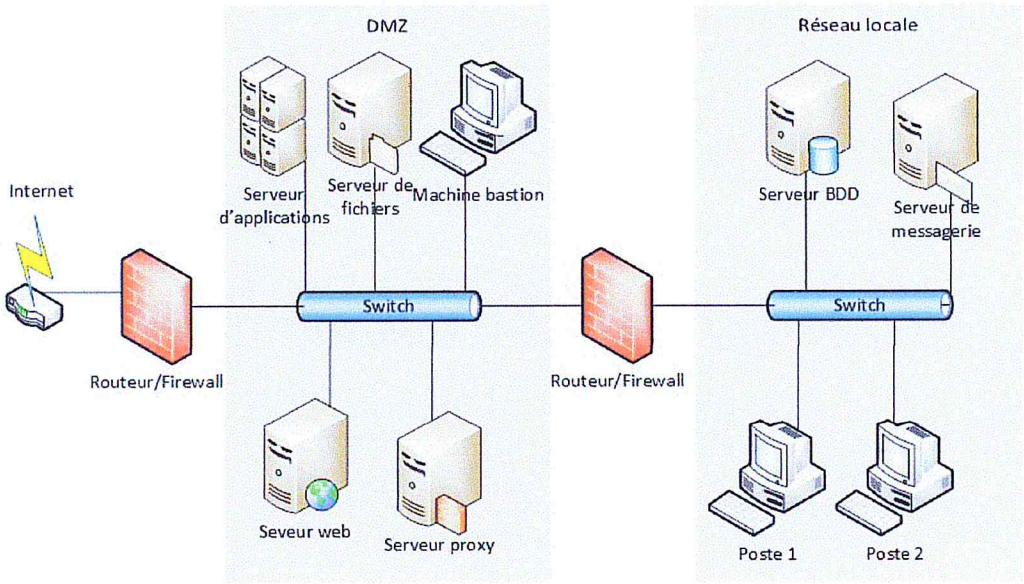


Figure 2.4 : DMZ entre deux firewalls

En effet, les pirates doivent franchir deux obstacles. Le trafic entrant est sécurisé une première fois par le routeur externe. Celui-ci est configuré pour repousser l'IP spoofing et gérer les accès Internet vers la DMZ.

Les utilisateurs externes n'ont donc accès qu'au bastion host et aux serveurs publics de la DMZ. Le second routeur n'autorise pas vers le réseau privé que ce qui provient du bastion host. Le routeur externe n'accepte vers internet que ce qui provient du bastion host.

3.3.2 Firewall à trois interfaces :

Cette architecture est composée de :

- Un réseau local appelé aussi zone de confiance dont on place que des clients du réseau et des serveurs qui sont inaccessibles depuis le net. Aucune connexion ne peut être initiée depuis le net vers cette zone.
- Une DMZ contient les serveurs accessibles depuis internet et aussi depuis le réseau privé.
- Le firewall/routeur se charge ici de deux principales fonctions. La première c'est le routage pour permettre aux paquets de passer d'une zone à l'autre alors que ces zones ne sont pas situées dans le même réseau IP. La deuxième fonction est de filtrer le trafic entre diverses zones.

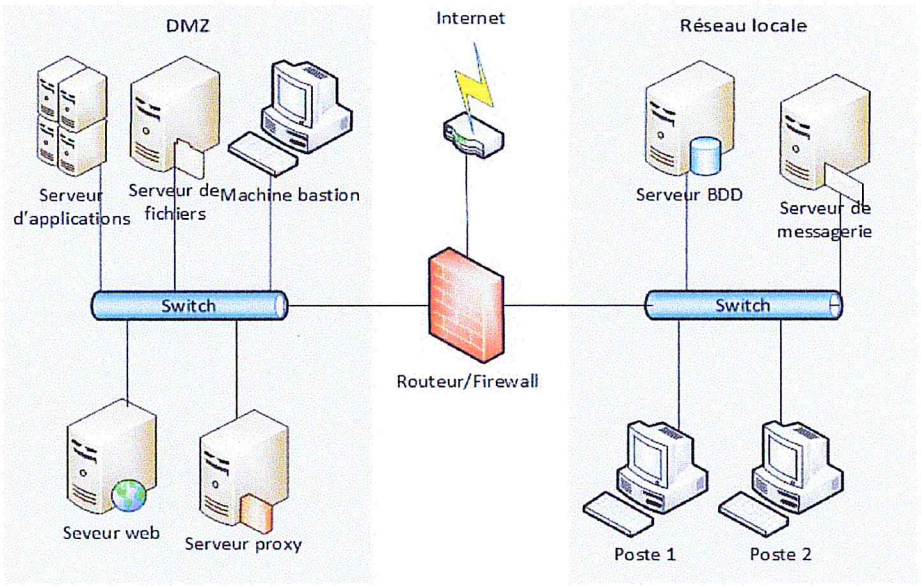


Figure 2.5 : Firewall à trois interfaces

On définit dans cette architecture trois types de communications qui seront soumis à des règles de passage différentes par le biais du firewall.

- Le passage entre le réseau local et le net :

Toutes les requêtes partent du réseau local vers le net. Seules les réponses à ces requêtes doivent entrer dans la DMZ. Les clients du réseau local n'ont aucun droit d'accès vers internet, ils ne peuvent consulter qu'un nombre de sites limités dans le cadre de leurs activités professionnelles exclusivement. Cette zone est construite sur une classe d'adresses privées et

nécessite donc une translation d'adresse pour accéder au net. C'est le routeur qui se chargera de cette translation.

- Le passage entre la DMZ et le net :

Dans la DMZ, on a les serveurs qui doivent être accessibles depuis le net. Un serveur web, un serveur de messagerie, un serveur DNS. Il faut donc permettre de laisser des connexions initiées depuis l'extérieur. Cela présente des dangers, il est recommander de surveiller et de ne laisser passer que le nécessaire. Dans le cas présent, on dispose d'une seule adresse ip publique, le routeur devra faire du « port forwarding » avec cette adresse pour permettre d'accéder aux autres serveurs de la DMZ. Cette technique fonctionne bien sur un petit nombre de serveurs.

- Le passage entre le réseau privé et la DMZ :

Ce passage nécessite une mise à jour des serveurs web et du contenu du FTP. Il faut ainsi envoyer et recevoir des messages puisque le SMTP est dedans. En revanche, depuis la DMZ, aucune connexion ne devrait initier vers la zone privée.

3.3.3 Comparaison entre les deux technologies :

Architecture	DMZ avec deux firewalls	Firewall à trois interfaces
Avantages	- Niveau de sécurité très élevé	- Un bon niveau de sécurité
Inconvénients	- Cout d'investissement élevé - Effort administratif important	- Le système comporte deux sécurités distinctes, le routeur et le proxy, si l'une des deux est paralysée, le réseau est menacé dans son intégrité

Tableau 2.1 : Comparaison d'architectures firewall avec DMZ

Malgré son cout d'investissement élevé et l'effort administratif nécessaire pour sa mise en place et son maintien, nous choisissons dans notre projet l'architecture DMZ avec deux firewalls pour le niveau de sécurité qu'elle peut apporter.

4 Types de firewalls :

Il existe trois types de firewalls, présentés dans ce qui suit :

4.3 Firewall matériel :

Un firewall matériel est une boite noire ou encore un équipement réseau qui repose sur une couche matérielle sur lequel un logiciel et des applications sont préinstallées, il est placé entre les réseaux locaux et éloignés, et autorise ou refuse les transferts en se basant sur des règles prédéfinies.

Bien qu'ils offrent un très bon niveau de sécurité et une simplicité de configuration ainsi qu'une bonne intégration avec les autres fonctionnalités du routeur. Néanmoins, ils sont totalement dépendants du constructeur du matériel pour les mises à jour, ce qui peut être assez contraignant. Seules les spécificités prévues par le constructeur du matériel sont implémentées. L'implémentation d'une autre fonction sur ce firewall est impossible. Il faut donc bien déterminer à l'avance ses besoins et choisir le constructeur du routeur avec soin.

4.4 Firewall bridge :

Un firewall bridge se trouve typiquement sur les Switch, d'où son appellation. C'est le type de firewalls relativement répandus. Ils agissent comme de vrais câbles réseau avec la fonction de filtrage en plus leurs interfaces ne possèdent pas d'adresse IP, et ne font que transférer les paquets d'une interface à une autre en leur appliquant les règles prédéfinies. Cette absence est particulièrement utile, car cela signifie que le firewall est indétectable par un hacker. En effet, quand une requête ARP est émise sur le câble réseau, le firewall ne répondra jamais. Ses adresses Mac ne circuleront jamais sur le réseau, et comme il ne fait que transmettre les paquets, il sera totalement invisible sur le réseau. Cela rend impossible toute attaque dirigée directement contre le firewall, étant donné qu'aucun paquet ne sera traité par ce dernier comme étant sa propre destination. Donc, la seule façon de le contourner est de passer outre ses règles de drop. Toute attaque devra donc essayer de contourner les règles.

Dans la plupart des cas, ces derniers ont une interface de configuration séparée. Un câble vient se brancher sur une troisième interface, série ou même Ethernet, et qui ne doit être utilisée que ponctuellement et dans un environnement sécurisé de préférence, (Chaouchi, 2015).

4.5 Firewall logiciel :

Un firewall logiciel est un logiciel installé sur une machine qui constitue la dernière barrière entre la machine et l'extérieur. Il est présent à la fois sur les ordinateurs, les serveurs et les routeurs.

Les firewalls logiciels ont pour avantage de savoir l'identité de celui qui ouvre un port de sortie et donc de gérer les autorisations application par application. En contrepartie ils reposent sur couche logiciel qui n'est parfois très stable et peut être contournée par ce biais et n'offrent pas un bon niveau de sécurité.

5 Fonctionnalités intégrées dans un pare-feu classique :

Comme évoqué précédemment le firewall sert d'interface entre le réseau interne et externe, sa principale fonction est de filtrer le trafic transitant le réseau interne sur les basiques des transferts réseaux, il possède d'une fonction de journalisation qui documente tous les paquets transitant le réseau ainsi que les actions effectuées, ce qui peut fournir des informations précieuses pour l'analyse et les statistiques ; Mais il se contente essentiellement de bloquer les paquets, de surveiller des ports et parfois d'offrir une protection contre les attaques DOS.

Néanmoins il implémente également d'autres fonctionnalités dont le domaine peut sembler connexe. Il partage avec le routeur certaines fonctionnalités, il permet d'une part le routage des paquets IP entre deux interfaces. D'autre part, il offre un certain niveau de sécurité pour le réseau interne étant donné qu'il camoufle complètement l'adressage interne à travers le mécanisme de translation d'adresses NAT appliqué en tant que paramètre général du pare-feu.

Il offre aussi la possibilité de création d'un VPN (réseau interne multi-site utilisant des tunnels chiffrant entre sites) aidant à la sécurisation de l'accès aux ressources internes des itinérants.

Il est à noter que le filtrage avec ses différents types, la journalisation, le routage ainsi que l'intégration de plusieurs mécanismes de sécurité au sein d'un firewall, se fait généralement au prix d'une consommation de ressources qui peut grever les performances globales pour cela il est préférable d'opter pour un firewall matériel robuste et performant, spécialement conçu pour remplir différentes fonctions.

6 Firewalls de nouvelle génération :

Les firewalls classiques, se sont longtemps limités à un simple filtrage de paquet. Pour une meilleure protection du réseau, les firewalls doivent traiter et analyser toutes les informations

contenues dans les paquets IP y compris les données. Ce qui a donné naissance à une nouvelle génération qui implémente des fonctionnalités beaucoup plus intéressantes.

6.1 Définition :

Un firewall de NextGen est un pare-feu applicatif, qui ne se base plus seulement sur les adresses IP et les protocoles pour filtrer un trafic réseau mais (au minimum) sur des identifiants utilisateurs et sur une liste d'applications autorisées. Pour mériter le qualificatif de « nouvelle génération » de firewall, l'équipement doit en plus montrer une capacité accrue d'analyse de contenu selon la technologie « Deep Packet Inspection » afin de repérer, en temps réel, les virus, malwares et autres menaces embarquées au sein du contenu.

6.2 Technologie DPI :

En effet, la technologie DPI mêle les fonctions des systèmes de détection (IDS) et de prévention (IPS) d'intrusions à celles d'un pare-feu à état : cette combinaison permet de détecter certaines attaques que les IDS/IPS et le pare-feu ne peuvent révéler à eux seuls. Si le pare-feu à état peut voir le début et la fin d'un flux de paquets réseau, il ne peut pas remarquer des événements inadéquats pour une application en particulier. Les IDSs peuvent détecter les intrusions, mais sont peu utiles pour les bloquer ; enfin les DPI sont employés pour prévenir les attaques par virus ou vers, et s'avèrent plus spécifiquement utiles contre des attaques par dépassement de tampon, par Déni de service (DoS), ou par l'emploi de vers qui tiennent dans un seul paquet.

Le DPI permet de lire toutes couches du Modèle OSI, ce qui inclut à la fois les headers (en-têtes), les structures des protocoles et la charge, le contenu du message lui-même. Il peut par ailleurs identifier et classer le trafic à partir d'une base de données de signatures, c'est-à-dire à partir des données contenues dans le paquet lui-même. Un chiffrage des points de sortie est donc généralement nécessaire pour échapper à une inspection de type DPI. Un paquet classifié peut être redirigé, marqué/taggé, bloqué, voir son débit limité, et bien sûr être rapporté à un agent du réseau. Dans ce genre de cas, plusieurs types d'erreurs HTTP peuvent être identifiées et transférées pour une analyse ultérieure. Beaucoup de dispositifs DPI peuvent analyser des flux de paquets (plutôt que procéder à une analyse paquet par paquet), ce qui permet un contrôle sur des flux cumulés d'informations.

6.3 Fonctionnalités avancées :

Un pare-feu « nouvelle génération » combine les fonctionnalités d'un pare-feu classique avec un ensemble d'autres boucliers défensifs autrefois commercialisés séparément, à commencer par un IPS intelligent et une protection anti-malware avancée. En embarquant ainsi davantage

d'intelligence, ils permettent de simplifier l'infrastructure en limitant la multiplication d'outils indépendants, à l'administration difficilement centralisée. Parmi les fonctionnalités intégrées on peut distinguer :

a. **L'IPS** :

Tous les UTM/NGFW intègrent un système de prévention et de détection d'intrusion (IPS/IDS) s'appuyant en général sur un mécanisme de règles et de signatures prédéfinies. Il décode les protocoles, et réalise de l'inspection approfondie des paquets afin de surveiller les flux entrants/sortants et reconnaît les actions potentiellement dangereuses ainsi que les attaques les plus typiques.

b. **Le blocage par géolocalisation des IPs** :

C'est de n'autoriser le contrôle à distance que depuis les pays que les collaborateurs visitent, ou l'accès au serveur FTP que depuis les pays où l'entreprise a des clients dans le monde.

c. Gestion par réputation :

Cette défense consiste généralement à bloquer l'accès aux IP et aux URLs de sites connus comme dangereux ou potentiellement dangereux. Certains appareils étendent la notion de réputation aux fichiers et même aux emails. L'idée consiste alors à bloquer automatiquement les fichiers et emails entrants provenant de sources inconnues et présentant des aspects douteux (réputation des liens intégrés, réputation du contenu, structure typique d'une menace, réputation des éléments attachés). Certains appareils vous permettent de définir vos propres règles de réputation.

d. Contrôle applicatif :

L'une des grandes particularités des NGFW est de comprendre la notion d'application, l'email, mais aussi les messageries instantanées, la téléphonie IP, la téléconférence, le multimédia en streaming, les applications P2P, les réseaux sociaux ou même les recherches Web sont devenus des vecteurs potentiels de menace et des canaux d'attaque. Les NGFW aident à filtrer (et contrôler) les usages professionnels et hors professionnels de ces applications mais aussi à parer certaines attaques en vérifiant la légitimité d'utilisation de ces applications en fonction des utilisateurs et de leur contexte de connexion.

e. Bouclier Anti-DDOS :

Les attaques par déni de service sont un grand classique. Pour ceci NGFW fournissent des filtres spéciaux et combinent les boucliers IPS, Réputation et Géolocalisation des IP pour nettoyer les flux entrants, jeter les paquets provenant de sources indésirables et réduire l'impact des attaques.

f. Antivirus et détection APT :

Aujourd'hui quasiment tous les NGFW embarquent un antivirus intégré (de plus en plus directement relié à une intelligence Cloud pour éviter les téléchargements de signatures) afin de détecter et bloquer les malwares et les APT. Certains sont même capables de détecter non pas uniquement les fichiers mais aussi les activités typiques des APT par une analyse de comportement.

g. Antispam :

Ils intègrent aussi un antispam. Celui-ci analyse tous les emails entrant et élimine automatiquement ceux réputés comme dangereux soit parce qu'ils contiennent une pièce attachée vérolée, soit parce qu'ils contiennent un lien vers un site de phishing ou d'attaques par exploits.

h. Fonction DLP :

Ils disposent également d'une fonctionnalité qui interdit à certains utilisateurs de transférer des informations sensibles (numéro de carte bancaire par exemple) ou qui bloque les conversations, les recherches ou l'accès à des sites en fonction de mots clés.

i. Contrôle des accès mobile et VPN :

Aujourd'hui les accès au système d'information depuis « l'extérieur » sont indispensables et permanents. La mobilité engendre des problématiques de sécurité nouvelles et supplémentaires. Il est essentiel de permettre un accès sécurisé à l'entreprise et de pouvoir surveiller, contrôler et gérer efficacement ces accès.

j. Contrôle des utilisateurs :

Ils savent aussi contrôler les utilisateurs et permettent de définir des règles en fonction de l'utilisateur. C'est évidemment essentiel pour personnaliser les contrôles applicatifs et les contrôles d'accès mobiles en fonction des catégories d'utilisateurs. Mais il devient ainsi

possible de combiner géolocalisation, application, trafic et utilisateurs pour mieux discerner les activités suspectes.

k. Outils de visualisation temps-réel :

Ils offrent des outils de visualisation en temps réel des activités douteuses et des menaces. D'autres permettent de façon visuelle de connaître à tout moment et en temps quel utilisateur ou quel terminal utilise quelle application (ou quelles sont ses activités). Ces outils peuvent aussi se révéler très utiles pour aider à la configuration du pare-feu ou pour analyser des problèmes de connectivité. « Savoir, c'est déjà en partie se protéger ».

7 Les UTMs :

7.1 Définition :

La plupart des analystes de l'industrie définissent les pare-feu de nouvelle génération comme des pare-feu améliorés avec prévention des intrusions et contrôle des applications, et les systèmes de gestion des menaces unifiée (UTM) comme incluant ces fonctions plus d'autres technologies telles que la sécurité de la messagerie, le filtrage des URL, la sécurité sans fil, les pare-feu d'applications Web et les réseaux privés virtuels (VPN). Selon cette définition, le pare-feu de nouvelle génération est donc un composant du système UTM.
Cependant, de nombreux individus utilisent ces termes indifféremment et certains éditeurs UTM commercialisent leurs produits haut de gamme comme des pare-feu next-gen. Mais ne nous arrêtons pas à une question de pure terminologie. Si nous utilisons des pare-feu next-gen dans le sens large du terme, alors les points abordés ci-dessous représentent les technologies de sécurité s'appliquant aussi bien aux systèmes UTM qu'à certains firewalls de nouvelle génération.

7.2 Technologies de sécurité intégrées :

Le tableau ci-dessous résume ces technologies de sécurité. De nos jours presque tous les éléments sont intégrés dans les systèmes UTM avancés. Les entreprises n'ont pas besoin de déployer toutes les technologies d'un seul coup. Avec la plupart des systèmes UTM, elles peuvent choisir d'implémenter les défenses dont elles ont besoin pour un début et d'en activer d'autres plus lorsqu'elles deviennent nécessaires.

Catégorie	Technologie de sécurité
Protection réseau	• Pare-feu dynamique • Traduction d'adresses réseau • Système de prévention des intrusions • Protection contre les inondations (blocage, portscan, DoS, DDoS) • Authentification à deux facteurs • Accès à distance et VPN de site à site
Protection web	• Filtrage des URL • Protection contre les logiciels espions • Contrôle antivirus du trafic Web • Contrôle HTTPS
Protection de la messagerie	• Détection antispam • Mise en quarantaine des messages suspects • Contrôle antivirus des pièces jointes dans les emails • Chiffrement des emails et prévention des pertes de données (DLP)
Protection des serveurs web	• Pare-feu d'applications Web et reverse proxy • Contrôle antivirus pour les téléchargements du Web • Durcissement au niveau des formulaires • Durcissement au niveau des URL • Utilisation des cookies
Protection WIFI	• Contrôle du trafic câblé et du trafic sans fil • Chiffrement WPA et WPA2 • Zones sans fil séparé pour les accès invités • Options d'authentification hotspot
Protection des systèmes d'extrémité	• Analyse antivirus sur les systèmes d'extrémité • Contrôle des périphériques pour prévenir le branchement de périphériques à risque (tels que les clés USB) et les connexions réseau (par exemple le Bluetooth) • Prévention des fuites de données (DLP)

	• Protection Web pour les utilisateurs itinérants
Pare-feu de nouvelle génération (next-gen)	• Visibilité et contrôle des applications • Protection avancée contre les menaces • Qualité de service et contrôle de la bande passante

Tableau 2.2:Technologies de sécurité par type de protection

8 Synthèse :

Selon l'étude menée, le pare-feu de nouvelle génération possède toutes les fonctionnalités d'un pare-feu classique, et montre de plus une capacité accrue d'analyse de contenus. L'UTM quant à lui est un NGFW avancé qui inclut différentes technologies de sécurité commercialisés séparément. Pour cela, dans notre projet nous optons pour l'utilisation d'un firewall UTM.

9 Conclusion :

Dans ce deuxième chapitre nous avons présentés les concepts fondamentaux des firewalls. Outre les définitions nous avons eu une vue d'ensemble sur les différentes architectures firewalls, les types de filtrage et les types de firewalls utilisées, puis nous sommes passés aux fonctionnalités supplémentaires (en plus du filtrage sans état et le filtrage à état) pouvant être effectuées par un firewall classique à l'insu des performances souhaités.

Ensuite nous nous sommes intéressés aux pare-feu de nouvelle génération, pour comprendre leurs particularités et les fonctionnalités qu'ils proposent ; notre étude s'arrête au niveau des UTMs la dernière arme dans l'arsenal défensif pour survoler les dernières technologies de sécurité intégrées dans les systèmes UTMs avancés.

Suite à cette étude qui nous a permis de cerner les concepts clés des firewalls, et dans le cadre de notre travail, nous consacrons le prochain chapitre à l'étude du système existant de la CNEP banque et les mesures de sécurité prise pour la protection du réseau, dans le but de proposer une solution spécifique adaptée aux besoins de l'entreprise, à partir des problèmes rencontrés.

Chapitre III : Analyse des besoins

1. Introduction :

Dans la première partie de notre mémoire, nous avons réalisés une analyse complète de l'état de l'art, relevant du domaine de la sécurité informatique et de la protection réseau à travers divers moyens de sécurité en détaillant particulièrement les firewalls.

L'objectif du présent chapitre est de proposer une solution de sécurité adaptée à l'entreprise. Autrement dit, une solution qui répond aux faiblesses de sécurité réseau actuelles d'une part, et d'autre part, prend en considération l'évolution de l'entreprise et son environnement. Pour cela, il s'avère nécessaire disposer d'informations sur l'infrastructure réseau de la banque, afin de comprendre le fonctionnement actuel du réseau informatique et aussi prendre connaissance des problèmes ayant une incidence sur la sécurité et la qualité des communications réseau.

Nous commençons par présenter l'étude élaborée sur le réseau de l'entreprise, comprenant son architecture et les moyens de sécurité mises en place, ensuite nous présentons les vulnérabilités existantes. Enfin, nous expliquons en détail la solution proposée.

2. Etude de l'existant :

L'étude élaborée est orientée au besoin du projet, elle porte sur deux principaux axes. Le premier axe est consacré à la description de l'architecture du réseau informatique de l'entreprise. Le deuxième axe quant à lui concerne les mesures de sécurité mises en place afin de protéger le réseau.

2.1.Description de l'architecture réseau :

La CNEP banque est doté d'un réseau informatique étendu sur le territoire national, il permet d'une part la communication entre la direction générale et les différentes directions régionales et agences de l'entreprise à travers son réseau intranet, et d'autre part, l'accès à internet dans le cadre des activités financières et bancaires, sans oublier la communication avec les banques partenaires à travers son réseau extranet.

Afin de permettre une bonne compréhension de l'architecture réseau de l'entreprise, nous présentons séparément l'architecture intranet et extranet dans les sous sections suivantes.

2.1.1. Architecture intranet :

La CNEP banque adopte pour son réseau informatique une architecture physique mixte, il s'agit d'une architecture hiérarchique en étoile étendue, elle est organisée en 3 niveaux :

- Niveau 1 : il s'agit du site principal de la direction générale, et un site de secours.
- Niveau 2 : il s'agit des sites des directions régionales.
- Niveau 3 : il s'agit des agences.

Dans le but d'avoir une vue d'ensemble sur l'intranet de l'entreprise, nous avons opté pour une représentation globale du réseau, **voir la figure 3.1**.

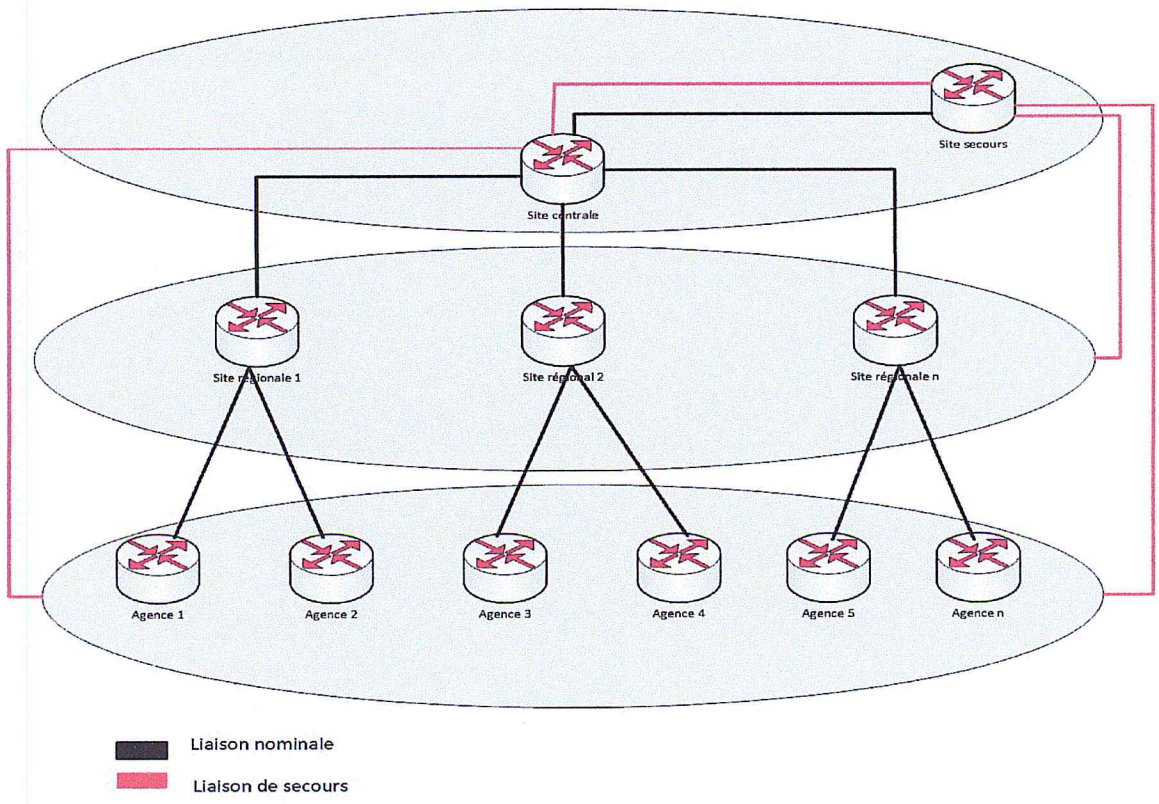


Figure 3.1: Architecture physique de l'intranet de la CNEP banque

Comme le montre la **figure 3.1**, on peut distinguer deux liaisons, à savoir une liaison nominale et une liaison de secours :

- La liaison nominale :

il s'agit de l'interconnexion entre le site centrale et les sites régionaux ainsi que celle des sites régionaux et agences, elle est effectué par une ligne spécialisée, permanente et exclusive pour éviter la saturation du réseau, et assurer un transfert de données rapide et sécurisée ainsi qu'une communication de qualité.

- La liaison de secours :

Il s'agit d'un deuxième raccordement, qui permet l'interconnexion du site de secours avec les sites régionaux et les agences, ainsi que le site de secours au site central, il est effectué par une liaison RMS (Réseau Multiservices) fournit par le même FAI (Algérie Telecom). Cette redondance limite les risques d'interruption et garantit la continuité des services.

En effet, la liaison de secours fait partie intégrante du plan de continuité de services, et c'est dans ce même contexte que l'entreprise a eu recours à un site de secours. Il s'agit d'un site miroir distant, relié directement au site central par une liaison nominale ainsi qu'une liaison de secours. En cas de sinistre du premier site, le second prend instantanément le relais.

Cette approche assez connu dans le domaine de gestion des risques, offre un niveau de sécurisation plus élevé et apporte à l'entreprise des avantages compétitifs tant au quotidien, qu'en situation de crise, car elle permet de rassurer les clients et partenaires de la résilience de la banque qui se traduit par une stabilité commerciale en toutes circonstances ; ainsi que la tolérance aux interruptions, qui maintien des activités critiques à un niveau acceptable prédéfini, et préserve alors les parts de l'entreprise au marché.

La conception de réseau hiérarchique en étoile implique la division du réseau en trois couches distinctes : couche core, couche distribution et couche accès. Et puis la convergence des hôtes finaux vers l'équipement central d'interconnexion (Switch d'accès). Ce qui permet d'avoir une gestion relativement simple et centralisée, et offre un bon niveau de sécurité.
La figure 3.2 fait référence à l'architecture réseau d'un des sites de l'entreprise.

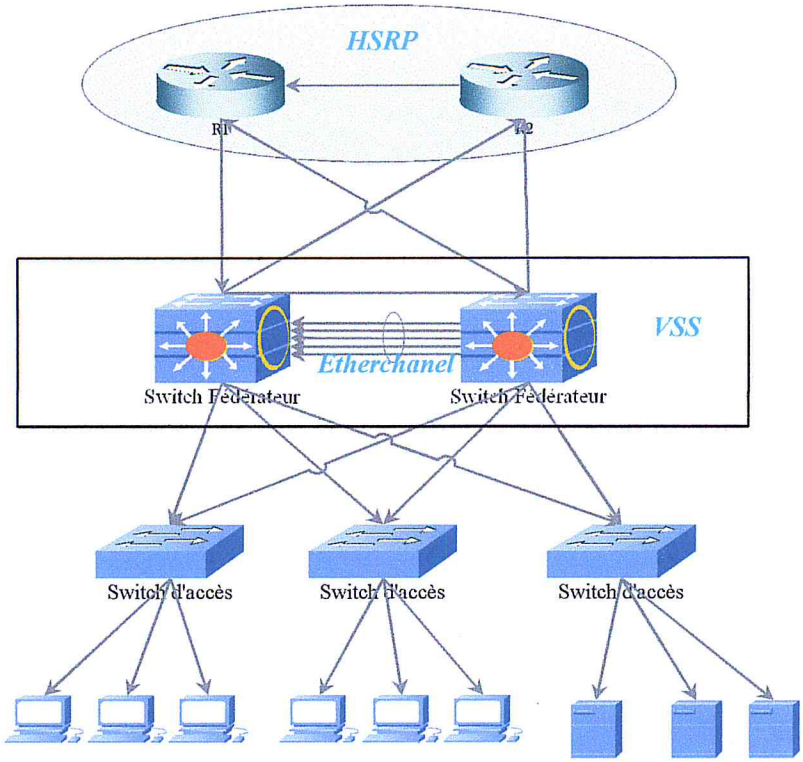


Figure 3.2: Exemple de l'architecture LAN d'un site

Etherchanel : est une technologie d'agrégation de liens utilisés principalement sur les commutateurs de Cisco.

HSRP: est un protocole propriétaire de "continuité de service" implémenté dans les routeurs Cisco pour la gestion des "liens de secours".

VSS: est une technologie de virtualisation de système de réseau disponible les commutateurs Cisco.

Hormis la sécurité et la facilité de gestion, l'utilisation de cette topologie réseau a permis de bénéficier des avantages suivants :

- Evolutivité : les réseaux hiérarchiques peuvent être aisément étendus. La modularité permet de reproduire des éléments au fur et à mesure de l'évolution du réseau.
- Performance : la performance des communications entre les sites distants s'améliore en évitant de transmettre les données via des commutateurs intermédiaires peu performants.
- Redondance : La redondance au niveau des couches principales et de distribution garantit la disponibilité des chemins d'accès.

Parallèlement à l'architecture physique, l'entreprise adopte une architecture logique client-serveur, pour permettre une administration centralisée des ressources de l'entreprise, **voir la figure 3.3**.

En effet, les ressources sont placées au niveau du site central, au data center, les agences y accèdent, à travers une liaison virtuelle, les données sont véhiculées en toute sécurité grâce à un tunnel VPN, détaillé dans la section d'après.

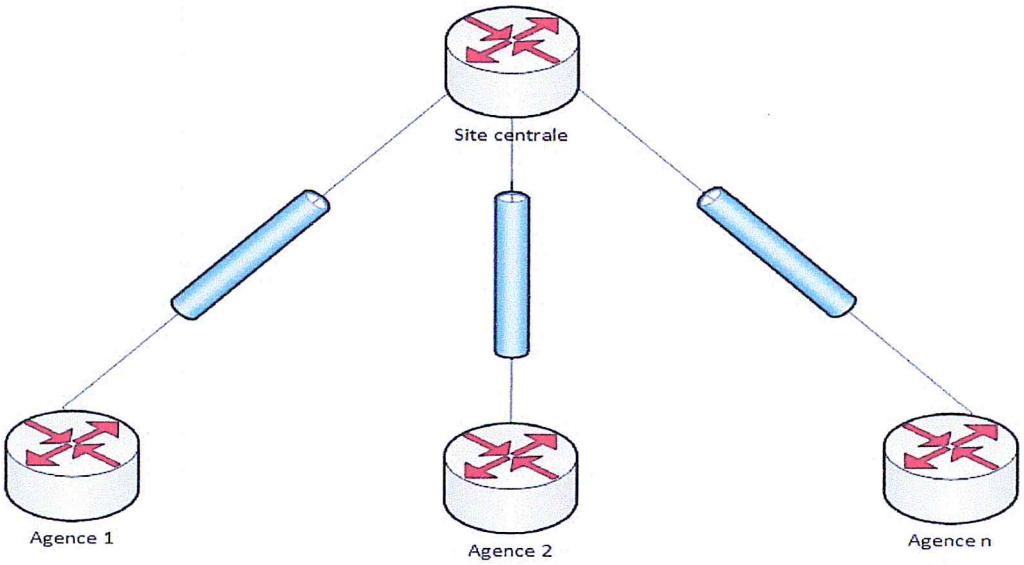


Figure 3.3 : Architecture logique du réseau de la CNEP banque

2.1.2. Architecture Extranet :

La figure 3.4 représente une architecture simplifiée de l'extranet de l'entreprise. C'est une architecture firewall avec une zone démilitarisée, en revenant à la partie état de l'art, au deuxième chapitre, on constate rapidement qu'il s'agit de la variante « firewall à trois interfaces ». Le réseau est scindé en deux parties : la DMZ et le réseau local.

Le réseau local lui-même est segmenté en deux sous réseaux. Le premier sous réseau regroupe les postes des utilisateurs, et le deuxième sous réseau constitue la partie la plus sensible de l'intranet, il s'agit du centre de données qui garde les données de tous les clients de l'entreprise. Ces données sont à caractère bancaire, d'où la nécessité d'une politique de sécurité solide.

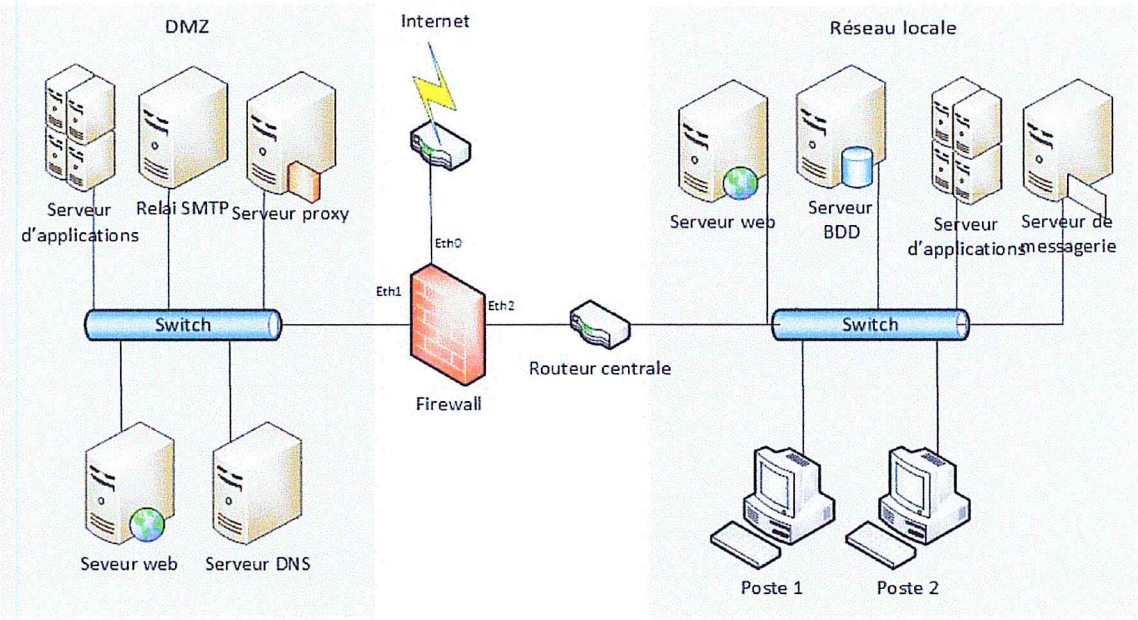


Figure 3.4 : architecture du site principal

Comme évoqué précédemment, la DMZ regroupe les machines accessibles depuis internet, pour le cas de la CNEP banque, L'accès n'est permit qu'aux clients de l'entreprise et ses deux partenaires, bien évidement qu'aux ressources informatiques dont ils ont besoins. Réseau local : cette partie du réseau est elle-même segmentée pour séparer le Data Center des postes utilisateurs.

Communication entre DMZ et LAN :

- DMZ vers LAN : pour la récupération des données, il est primordial que les serveurs publiques accèdent au réseau local, plus exactement au Data center.
- LAN vers DMZ : Pour se connecter à internet, les utilisateurs du réseau local passent obligatoirement par la DMZ. En effet, les machines internes et externes partagent le même serveur DNS, contrairement au serveur web, un est consacré aux machines internes et un autre aux machines externes, ce qui explique l'accès à la DMZ lors de toutes communications du réseau local vers l'extérieur au lieu de passer directement par l'interface eth2 à eth0.

Le serveur SMTP quant à lui, est partagé entre les machines internes (pour jouer le rôle de messagerie interne), et les machines externes (pour l'envoi et la réception de courriers électroniques vers/depuis l'Internet), c'est la raison pour laquelle il est mis dans la DMZ, et le flux va dans les deux sens.

On voit également la liaison avec le réseau public, à travers le routeur de l'opérateur qui joue le rôle de passerelle entre le réseau de l'entreprise et le réseau public. Le trafic entre les trois zones, à savoir internet, la DMZ et le réseau local, est contrôlé par un firewall classique. La liaison avec les directions régionales est effectuée à travers le routeur central.

2.2.Mesures de sécurité :

Après avoir découvert l'architecture réseau adoptée par la CNEP banque, à savoir l'architecture de l'intranet et celle de l'extranet, nous parvenons dans cette section à l'étude des mesures de sécurité réseau mise en place pour protéger au mieux son infrastructure.

2.2.1. Firewall :

Il s'agit d'un équipement matériel, dans notre cas c'est un firewall à trois interfaces, qui se trouve au niveau du site principal de l'entreprise, il contrôle le trafic réseau provenant de l'internet vers DMZ ou LAN, ou du LAN vers internet, il permet d'effectuer un filtrage sans état, en se basant sur les adresses IP et les numéros de ports configurés précédemment, ainsi qu'un filtrage à état en tenant compte du contexte de chaque connexion.

Il réalise également la translation d'adresses, dans sa version dynamique. Ce qui permet d'une part de fournir un accès internet aux machines internes, et d'autre part de dissimuler les adresses réellement utilisées en interne et donc offre une sécurité supplémentaire

Hormis, les fonctions de protection citées, ce firewall permet la Journalisation, une fonction complémentaire à celles de protection, dans le sens où elle fournit des informations précises sur tous les paquets, ce qui constitue un support important au moment d'une analyse, d'un audit …etc.

2.2.2. Système de prévention d'intrusion :

Il s'agit d'un N-IPS, intégré également au niveau du firewall pour repousser les tentatives d'intrusion au réseau, sa présence dans le site principal est primordial afin de détecter et de prévenir les actes malveillants ou anormales sur les principaux liens à savoir du LAN vers la DMZ ou l'extérieur ainsi que de l'extérieur vers la DMZ sur la base des signatures d'attaques déjà répertoriés.

2.2.3. Serveur proxy:

Il existe un serveur proxy qui se trouve dans la DMZ, voir **la figure 3.4.** Il faut noter que nous parlons ici d'un proxy http (appelé souvent serveur proxy web) Un filtre web qui analyse les URL sur la base d'une base de données qui associe des URL avec des catégories de contenus. Toutes les communications entrantes/sortantes du réseau extérieur passent par lui. Il est utilisé dans ce contexte pour :

- réaliser un filtrage de paquets sur le protocole http (filtrage web).
- garder dans le cache toutes les informations cherchées.

En effet, le proxy http apporte plusieurs avantages, il facilite la mise en place de la politique de sécurité réseau d'un côté, et contribue à l'optimisation de la bande passante sur le lien Internet, dans le sens où il bloque tout accès pour un usage non professionnel et en cas de demande d'une même information par plusieurs utilisateurs le téléchargement ne s'effectue qu'une seule fois.

2.2.4. Réseau Virtuel Privé :

Il s'agit d'un VPN routeur-à-routeur, également appelé VPN site-à-site, Comme c'est le cas pour beaucoup d'entreprises possédant des sites géographiquement éloignés, et désirent maintenir des communications sécurisées et privées entre ses différents sites. La CNEP banque s'en sert pour relier le site principal aux agences, ce qui construit un réseau virtuel. Le protocole VPN utilisé pour sécuriser les communications est IP sec, en mode tunnel.

Ce VPN est basé sur Intranet. Toutefois il n'y a pas de ligne dédiée, le routage, le cryptage et le décryptage sont effectués grâce aux routeurs situés des deux côtés.

2.2.5. Protection DOS :

La fonction de protection DOS est activée au niveau du routeur internet, pour filtrer et neutraliser les paquets suspects provenant de l'extérieur. Cette fonction est d'une grande importance, car elle permet d'éviter la surcharge de la bande passante WAN ou LAN, ou encore l'épuisement des ressources systèmes, et donc protège des attaques DOS les plus répandues.

2.2.6. QoS :

Autrement dit la qualité de service, la fonction dédiée à la gestion du trafic réseau. Les règles de QoS sont activées au niveau de tous les routeurs du réseau, elles sont bien évidemment indispensables tant pour la gestion du trafic d'intranet que pour la gestion du flux de l'extranet, car les connexions sont massivement partagées.

L'objectif est principalement d'optimiser les flux sur une connexion et donc s'assurer de la qualité des communications, elle participe également au maintien des latences acceptables en s'assurant qu'un trop grand nombre de paquets n'est pas en train de s'accumuler à l'entrée du réseau du fournisseur d'accès.

2.3.Mesures de sécurité complémentaires :

Notons au passage qu'en plus des mesures de sécurité réseau, le système est protégé de manière complémentaire par d'autres solutions de sécurité, à savoir : une solution antivirus, une solution antispam, filtres applicatif pour protection des applications et bien d'autres.

3. Vulnérabilités :

Grace à l'étude précédente il devient plus aisé de déterminer les problèmes qui ont une incidence sur la sécurité et la qualité des communications au niveau de l'intranet aussi bien que l'extranet de la CNEP banque, les critiques peuvent être organisées et présentées comme suit :

3.1 Firewall :

Le firewall existant se limite à un simple filtrage de paquets, à savoir le filtrage à état et le filtrage sans état qui reposent sur des critères basiques de sélection. Il n'a aucune capacité d'analyse de contenu du paquet, par conséquent il ne permet ni le contrôle des flux applicatifs ni la détection des menaces web, des menaces avancées (APT) ou toutes autres menaces embarquées au contenu.

Le contenu constitue un vecteur potentiel de menaces et un canal d'attaque très efficace. Quelque soit le contenu : applications web, emails, messagerie instantanée, réseaux sociaux ou encore sites web. Il peut véhiculer des virus, des spams, pièces attachées vérolées, sites de phishing, en plus de la consommation en bande passante.

Au niveau de l'intranet il y a une absence totale du firewall, il n y a pas une gestion du trafic inutile ni du trafic à risque entre les sites, et donc pas de contrôle d'accès réseau.

En effet le trafic inutile conduit à la surcharge des liaisons, et altère ainsi la qualité des communications au détriment des communications et usages professionnels.

Quant au trafic à risque, il est plus dangereux, il peut s'agir d'un virus en propagation, ou d'une attaque provenant de l'intérieur du réseau...etc., Dans la plupart des cas il est résultant d'une complicité interne à l'organisme. L'impact peut être fatale surtout si le trafic est en direction du site principal et/ou visant le centre de données qui garde des données bancaires extrêmement sensibles.

3.2 Système de prévention d'intrusion :

La présence d'un système de prévention d'intrusion se fait désirer surtout dans l'extranet mais sa mise en place comme un module intégré au firewall est un problème dans ce cas, car l'entreprise possède un firewall classique qui n'est pas aussi robuste, son moteur IPS augmente la consommation des ressources et surcharge le firewall. De plus il n'est pas doté d'un analyseur de comportement pour détecter les attaques non répertoriés, il ne détecte d'attaque que lorsque le paquet correspond à un modèle de signature (attaques répertoriés).

3.3 Proxy :

Le serveur proxy effectue un filtrage d'url sur la base de la catégorie du site visité, il ne permet pas d'effectuer un filtrage par contenu, par mots-clés ou un filtrage d'image, car il est incapable d'analyser le contenu du site web. Par conséquent, il ne peut pas détecter les sites non catégorisés, les sites tout neufs ou les sites récemment devenus malicieux.

En plus, il ne prend pas en charge la notion d'application ce qui empêche le contrôle et le filtrage les applications web.

3.4 WAF :

L'entreprise dispose d'applications métiers au format web, malgré la qualité de leur code source, l'absence d'une solution WAF entre l'utilisateur final et le serveur web exposent les applications à un grand nombre d'attaques (les plus connues, comme XSS, injections SQL, vols de session, attaques brute-force, etc.) surtout avec le développement des attaques web, qui deviennent de plus en plus sophistiqués et peuvent provenir même de l'intérieur de l'entreprise.

3.5Routeurs :

Quant au routeur d'internet, il est trop surchargé, en plus du routage et de la gestion de bande passante, il est prévu pour la protection des attaques DOS, une fonction de sécurité accomplit par un équipement dédié au routage de paquets IP sur un réseau qui reçoit des milliers de paquets par jour, ce qui ralenti les communications provenant de l'extérieur.

C'est le cas aussi pour les routeurs de l'intranet. Ils sont surchargés cette fois ci par le tunnel VPN crée entre les agences et le site principal. En effet, les fonctions de chiffrage et déchiffrage consomme en ressources matériels, logiciels et aussi le facteur temps ce qui conduit aux mêmes problèmes que le routeur d'internet.

3.6Redondance :

L'absence de redondance du firewall et du routeur internet, pose un problème au niveau de l'extranet, car c'est le point central par lequel l'ensemble des flux externes transitent, il s'agit d'un SPOF ou point individuel de défaillance. La panne d'un de ces deux nœuds entraîne une indisponibilité réseau et un arrêt des services. Les dégâts peuvent être fatals surtout que les deux équipements sont directement exposés à internet.

L'intranet aussi connait un problème de redondance, cette fois-ci au niveau des liaisons. La présence d'une liaison nominale et une liaison de secours du même type et du même fournisseur d'accès internet (Algérie télécom), constitue un risque. En cas de panne dans toute la liaison filaire le réseau intranet devient in-opérationnel.

4. Problèmes d'administration de la sécurité :

D'un point de vue gestion et administration de la sécurité, les administrateurs rencontrent de nombreux problèmes dans leur activité au quotidien, nous citons :

- Difficulté de la mise en place de la politique de sécurité, faute d'outils adaptés
- Plusieurs interfaces et consoles d'administration
- Difficulté de gestion des problèmes de sécurité à cause de l'incompatibilité entre les différents modules.
- Edition de rapports séparés qui donnent peu de vision globale sur la sécurité du réseau.

5. Solution proposée :

Pour tenter d'améliorer la sécurité du réseau informatique de la CNEP banque, il est important de choisir un moyen offrant une protection complète et un niveau de sécurité élevé. Ce moyen doit permettre le filtrage des paquets en profondeur avant même qu'ils transitent au réseau sans qu'il y ait une dégradation de la qualité et des performances des communications, afin d'éliminer toutes les menaces mêmes celles embarquées au contenu et avoir une possibilité de contrôle du flux applicatif.

Cependant, les moyens de sécurité réseau existants sont limités, ils ne répondent pas aux exigences indiquées auparavant, pour pouvoir fournir le niveau de sécurité souhaité. De ce fait, nous proposons d'opter pour la mise en place d'une solution firewall de nouvelle génération adoptant une approche unifiée de gestion des menaces.

Du fait qu'il s'agit d'un système informatique préexistant, le firewall reste la meilleure solution. En effet, ce type d'équipement présente l'avantage d'être indépendant des systèmes informatique déjà présents, qu'il s'agisse de serveurs d'applications, de serveurs de fichiers, ou d'équipements d'interconnexion réseaux. Cette autonomie présente un avantage à la fois du point de vue technique mais aussi du point de vue de l'administration et donc par rapport à l'organisation du service informatique.

Quant au concept de gestion unifiée des menaces (UTM), il est à la mode de nos jours. Les firewalls UTMs sont actuellement les outils les plus couramment utilisés de l'arsenal de sécurité de l'information, par rapport à l'approche utilisée auparavant (non unifiée), ils intègrent de nombreuses technologies de sécurité sur une seule plate-forme et fournies par un seul éditeur.

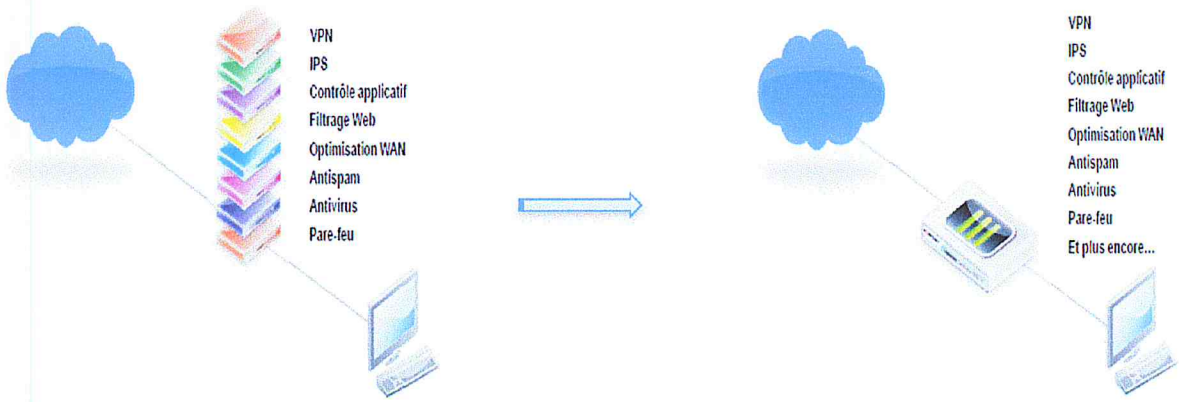


Figure 3.5 : passage à une approche de gestion unifiée des menaces

Hormis, l'utilisation des UTMs permet :

- Un déploiement simplifié, avec beaucoup moins d'étapes au niveau de l'installation et de la configuration ;
- Une administration facilitée car il n'y a qu'une seule console d'administration et un seul processus de mise à jour ;
- Une résolution plus rapide des problèmes car il y a moins de possibilités de conflits entre les modules et le support est assuré par un seul et même éditeur ;
- Des rapports intégrés qui regroupent toutes les données des différentes technologies à un seul endroit, dans un format homogène, avec des corrélations utiles entre les différents types de données.

Par rapport à l'entreprise, ces avantages techniques présentent des bénéfices concrets pour l'entreprise :

- Des coûts d'implémentation réduits
- Moins de pression sur le personnel informatique
- Moins de vulnérabilités de sécurité
- Des réactions aux attaques plus rapides

Des coûts administratifs réduits, du fait que les licences, la facturation et le support proviennent de la même source.

5.1 Proposition d'une architecture réseau :

L'ouverture du réseau de l'entreprise vers internet pour répondre aux besoins stratégiques de l'entreprise, l'expose encore plus aux cyberattaques. Ce qui nécessite le renforcement davantage de la sécurité du réseau extranet. Pour cela, en plus de la solution firewall UTM, nous proposons de mettre en place une nouvelle architecture de sécurité pour l'extranet offrant une haute disponibilité afin garantir la stabilité de l'entreprise et la continuité de ses services.

Dans les deux sous-sections suivantes, nous détaillons l'architecture extranet proposée, ensuite nous présentons le changement apporté à l'architecture intranet.

5.1.1 Architecture extranet :

Nous proposons d'adopter une architecture DMZ avec deux firewalls (une variante de l'architecture firewall avec DMZ) qui fournit un niveau de sécurité meilleur que celle utilisée auparavant, car le réseau admet deux barrières. En effet, le premier firewall gère les accès Internet et le deuxième gère les le trafic provenant de l'intranet.

Ainsi, le flux entrant d'internet au réseau local est contraint à traverser les deux firewalls l'un après l'autre pour profiter de la sécurité accrue offerte par l'architecture, comme le montre **la figure 3.6**.

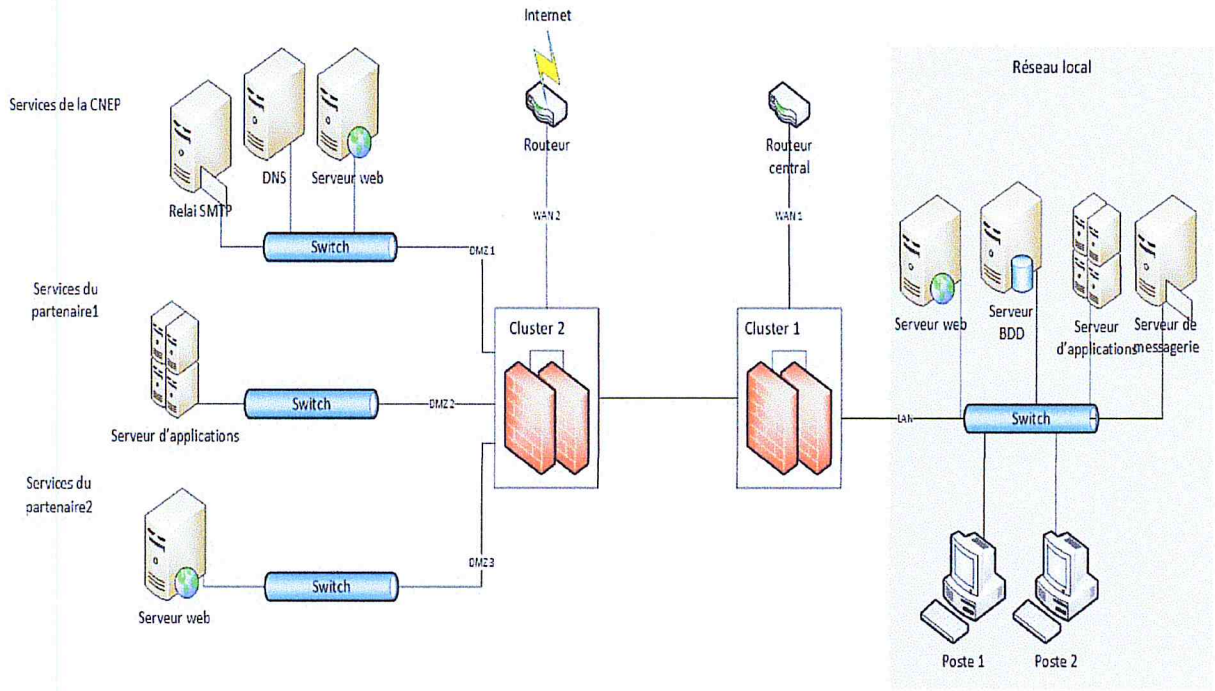


Figure 3.6 : Nouvelle architecture firewall pour l'extranet

Les serveurs publics sont de sensibilités différentes, il est donc préférable de ne pas les faire cohabiter sur le même réseau, nous proposons de partitionner la DMZ en trois sous réseau, les serveurs sont placés dans différentes DMZ en fonction du niveau de sécurité souhaité pour chacun d'entre eux. La sensibilité du serveur dépend des services proposés, qui peuvent être classés comme suit :

- Services dédiés aux clients.
- Services dédiés au premier partenaire.
- Services dédiés au deuxième partenaire.

Le besoin de forte disponibilité pour les services réseaux offerts par l'architecture, et notamment les services Web accessibles depuis Internet conduit à la mise en place d'une architectures dites de « haute disponibilité » impliquant deux équipements firewall. Toutefois, ils doivent être deux équipements de même type, et dotés d'un logiciel et de connexions réseau spécifiques, dédiées à la gestion de la redondance.

Pour répondre au besoin de disponibilité, les deux firewalls fonctionnent en mode de redondance passive (ou secours chaud). A un instant donné, l'un des deux équipements assure les fonctions de filtrage et de protection tandis que l'autre se tient prêt à prendre le relais en cas de défaillance du premier. L'équipement de secours dispose d'une version à jour de la liste de toutes les règles, ainsi qu'une version des tables d'états gérées dynamiquement par le firewall pour le suivi des connexions en cours. (Les deux équipements disposent également d'un moyen pour se surveiller mutuellement).

Ces différents besoins sont généralement remplis par la mise en place d'une connexion réseau directe entre les deux firewalls, identifiés sur **la figure 3.6**. Bien évidemment, toutes les connexions réseaux reliant les DMZs sont également doublées de manière à permettre à chacun des deux firewalls d'assurer le filtrage.

Outre l'accroissement de la protection du filtrage de sécurité par rapport à des défaillances accidentelles, la redondance aide également dans la réalisation de certaines opérations d'administration en deux étapes successives sans interruption du service : par exemple, la mise à jour du logiciel des firewalls.

Avec cette solution, dans certains cas, nous pouvons opter pour une redondance active (ou « partage de charge ») en faisant fonctionner simultanément les deux firewalls pour répartir les flux réseaux entre eux. Dans ce cas, les capacités maximales de traitement de l'architecture de sécurité peuvent être accrues (hors défaillance bien entendu, ce qui est un point généralement négligé). Toutefois, il nous semble que cette solution s'écarte parfois du besoin original en confondant quelque peu les questions de performance et de disponibilité.

5.1.2 Architecture intranet :

Pour bien accomplir leur fonctions, les firewalls sont positionnés au niveau des interconnexions entre les sites de l'entreprise, ce qui présente un avantage en terme de sécurité aussi bien qu'en terme de qualité et performances des communications réseau.

En effet, la mise en place d'un firewall à l'entrée de chaque site permet de pallier aux problèmes identifiés précédemment. Ils permettent à la fois de protéger les sites des menaces internes en éliminant le trafic à risque, mais aussi d'alléger la charge sur les liaisons en éliminant le trafic inutile.

La figure 3.7 représente l'architecture de l'intranet après l'adoption des firewalls UTM.

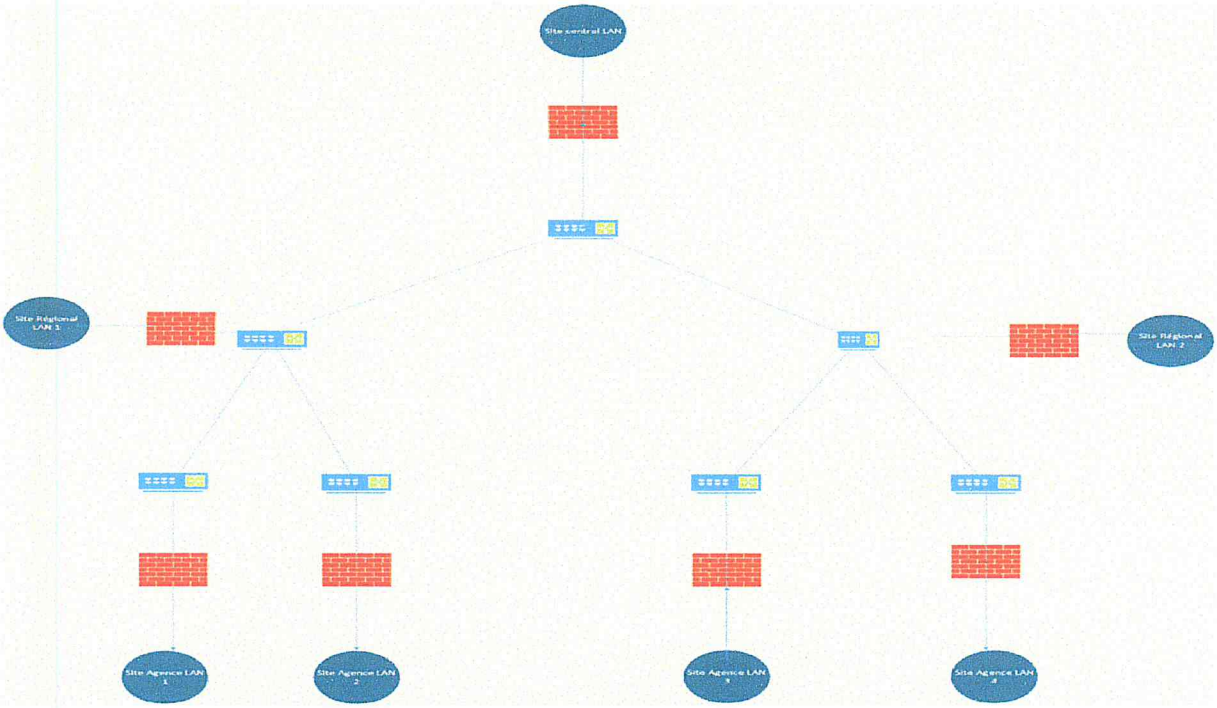


Figure 3.7 : Architecture intranet avec firewalls

5.2 Spécification de la solution :

Les technologies de sécurité disponibles dans les firewalls UTM sont nombreuses. Toutefois, les entreprises n'ont pas besoin de déployer toutes les technologies d'un seul coup. Avec l'adoption des firewalls UTM, la CNEP banque est libre d'implémenter les défenses dont elle a besoin maintenant selon la sensibilité du site et son exposition aux risques, puis d'en activer d'autres plus tard lorsqu'elles deviennent nécessaires.

L'utilisation des firewalls UTM est en mesure de remplacer tous les moyens de protection réseau existants au niveau de la banque, à savoir : le firewall, l'IPS intégré, le serveur proxy ainsi que les fonctionnalités activés au niveau des routeurs, et peut également remplacer (ou renforcer) les moyens de protection de la messagerie, du système, des applications et des serveurs web.

Nous choisissons d'implémenter toutes les fonctionnalités de protection dans les firewalls UTM pour différentes raisons, d'une part pour diminuer la charge sur les routeurs et éliminer

toutes les menaces susceptibles à l'entrée de chaque site, d'autre part pour ne pas ralentir le trafic (dans le cas où le paquet passe par des traitements différents, effectués par des équipements différents).

La protection du réseau de la CNEP banque, revient à la protection de l'intranet et de l'extranet en appliquant des mesures de sécurité différentes. Avec un firewall UTM nous procédons comme suit :

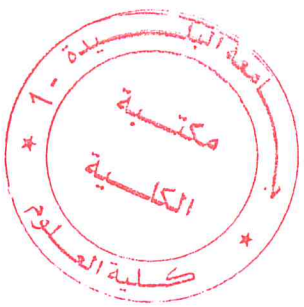
- Définition des Règles de sécurité pour la gestion de trafic au niveau de l'intranet (entre les différents sites de l'entreprise).
- Détection, réaction et gestion du trafic des applications web et des applications réseau de l'entreprise même si le trafic est encapsulé par d'autres protocoles.
- Détection et prévention d'intrusion appliqué sur tout le réseau, pour le protéger des attaques répertoriés et non répertoriés (attaques zéro day).
- Analyse antivirales de tous les paquets entrants/sortants des firewalls de l'intranet et l'extranet. Le scan est effectué sur tous les protocoles (FTP, HTTP, POP3, SMTP, IMAP…).
- Filtrage web statique et par catégorie effectué au niveau de l'extranet, pour se protéger des attaques web, et limiter l'accès internet qu'aux usages professionnels.
- Définition de règles DOS sur toutes les interfaces externes au réseau afin de réagir aux attaques DOS.
- Gestion de la bande passante LAN et WAN au niveau des firewalls plutôt qu'au niveau des routeurs.
- Mise en place d'un VPN IP sec au niveau de l'intranet (VPN site à site), entre les firewalls des différents sites plutôt qu'entre les routeurs afin de protéger les communications en interne.
- Mise en place d'un VPN SSL, pour protéger les transactions web et transmettre les données applicatives de manière sécurisée.
- Activation de la protection WAFs pour faire face aux menaces liées aux applications web.
- Filtrage des spams et gestion des mails commerciaux non sollicités.

6. Conclusion

L'étude nous a permis de comprendre le fonctionnement du réseau de la CNEP banque et les différentes solutions de protection réseau existantes ainsi que le niveau de sécurité qu'elles peuvent offrir et son impact sur la qualité des communications réseau. A partir de là, il était aisé de déterminer les problèmes ayant une incidence sur la sécurité réseau.

Par ailleurs, cette démarche nous a permis de prendre connaissance des exigences de sécurité nécessaire pour répondre aux diverses menaces. Suite à cela nous sommes arrivés à proposer une solution de sécurité solide, à savoir la proposition d'une nouvelle architecture firewall pour l'extranet ainsi que la mise en place d'un NGFW en adoptant une approche unifiée de gestion des menaces.

Dans la partie suivante, nous allons mettre en œuvre l'architecture de sécurité proposée et appliquer les mesures de sécurité définies en fin de ce chapitre dans un environnement de test, et finir par des tests dans le but de valider la solution proposée.



Chapitre VI : Déploiement, tests et validation

1. Introduction :

Après avoir exposé la solution de sécurisation avec ses deux volets, nous parvenons à la réalisation et validation dans le présent chapitre. Cette implémentation a impliquée la mise en cause de la démarche effectuée précédemment avant d'arriver à cette étape.

Pour expliquer la réalisation et le test de la solution proposée, nous commençons par présenter et motiver les outils utilisées pour sa mise en œuvre dans un environnement de test. Ensuite nous présentons la topologie de déploiement. Enfin, nous expliquons les étapes de déploiement du firewall, et configuration différentes technologies intégrées avec des images illustratives, suivi des tests réalisés et résultats obtenus.

2. Critères de choix d'un firewall NextGen :

La façon de configurer un Firewall et de le gérer est tout aussi importante que les capacités intrinsèques qu'il possède. Au moment du choix d'un firewall, il faut prendre en considération au minimum les critères suivants :

- La nature, le nombre des applications appréhendées (FTP, messagerie, HTTP, SNMP, vidéoconférence, etc.).
- La facilité d'enregistrement des actions et des événements pour audits futur.
- Les outils et facilités d'administration (interface graphique ou lignes de commandes, administration distante après authentification de gestionnaire, etc.).
- Simplicité de configuration et de mise en œuvre.
- La disponibilité d'outils de surveillance, d'alarmes, d'audit actif.
- Possibilité d'équilibrage de charges et de gestion de la bande passante de réseau.
- L'existence dans l'entreprise de compétences en matière d'administration du système d'exploitation du firewall.
- le prix.

Le choix des fonctionnalités de protection est aussi important, chaque entreprise doit déterminer les technologies de sécurité qui seront pour elle les plus importantes, en fonction d'un certain nombre de facteurs :

- Les auteurs des attaques dont elle est le plus susceptible de faire l'objet : cybercriminels, pirates commandités, hacktivistes, employés en interne, etc.
- Le type de techniques que ces auteurs sont le plus susceptibles d'utiliser : virus et chevaux de Troie, attaques ciblées basées sur les méthodes d'ingénierie sociale, les dénis de service, les injections SQL, le cross-site scripting (CSS) et autres attaques sur les applications Web, l'interception des emails et des communications sans fil, l'abus de privilèges par les utilisateurs de l'entreprise, etc.
- Les données et les équipements qu'elle a besoin de protéger : par exemple les données bancaires et financières, les dossiers médicaux, la propriété intellectuelle ou encore les mots de passe système, les serveurs, les ordinateurs portables, les tablettes et les smartphones.
- Les conséquences de ces attaques et de ces fuites, comprenant notamment les pertes de revenu et la baisse de productivité, les sanctions imposées par la loi ou encore les frais liés à l'obligation de notifier toute fuite de données.

Elle devra également considérer la propension des employés à ouvrir la porte à certaines de ces attaques en s'adonnant à des comportements à risque tels que le fait de cliquer sur des liens dans les emails de sources inconnues, consulter des sites suspects ou encore utiliser des points d'accès sans fil publics non sécurisés. Avec des menaces aussi variées, et les comportements complices des employés, beaucoup d'entreprises doivent inclure une gamme importante de technologies de sécurité dans leur système UTM.

3. Environnement de travail :

Le choix des outils de la simulation de déploiement d'une solution pour le réseau informatique d'une entreprise est une tache critique, Plusieurs contraintes doivent être respectées, les plus importantes sont le facteur temps et les performances attendues.

Notre solution a été développée sous le système d'exploitation « Windows 10 professionnel » moyennant les outils suivants :

VMware Workstation :

VMware Workstation est un hyperviseur, autrement dit une plate-forme de virtualisation qui permet de faire cohabiter différents systèmes d'exploitation sur une même machine physique. Il intègre une gestion complète des périphériques ainsi que du son, de la vidéo, et de la prise en charge réseau, il est doté d'une grande stabilité et une compatibilité avec les différents OS du marché. C'est incontestablement la meilleure solution pour émuler une machine multiprocesseur en offrant des performances de premier ordre.

De plus, le site VMware Workstation propose un bon nombre de machines virtuelles téléchargeables, balayant une large gamme de systèmes, y compris des systèmes Windows.

Dans le cadre de notre travail, nous avons optés pour VMware Workstation dans sa version 12 PRO, la procédure d'installation est détaillée en annexe technique, voir la page. Nous nous y sommes servis pour le déploiement de l'émulateur réseau EVE NG.

EVE-NG :

EVE-NG est un émulateur réseau graphique, il s'agit de la nouvelle génération des émulateurs réseau du projet UNetlab (Unified Network Laboratory), qui supporte des images virtuelles, commerciales et open-source, multi vendeur, de différents équipements (routeur, switch, ips, ordinateurs…etc.). C'est d'ailleurs une version mise à jour de l'émulateur UNetlab. Son interface utilisateur graphique s'exécute dans un navigateur Web, l'accès est également possible à partir de la console.

Les utilisateurs peuvent créer des nœuds de réseau à partir d'une bibliothèque de modèles, les connecter ensemble et les configurer. Quant aux utilisateurs avancés ou administrateurs, ils peuvent ajouter des images logicielles à la bibliothèque et créer des modèles personnalisés pour prendre en charge presque tous les scénarios de réseau. Cet émulateur réseau s'exécute dans une machine virtuelle ou une machine linux afin de pouvoir configurer des ordinateurs Windows, Mac OS ou Linux.

EVE-NG avec sa version PRO constitue une plateforme prête pour répondre aux exigences informatiques actuelles, en offrant aux professionnels du réseau et de la sécurité d'énormes opportunités dans le monde des réseaux. Les options de gestion sans client permettent à EVE-NG PRO d'être le meilleur choix pour les ingénieurs d'entreprise sans influencer les politiques de sécurité de l'entreprise car il peut être exécuté dans un environnement complètement isolé.

Putty :

Putty est un émulateur de terminal UNIX qui permet de se connecter à distance à une machine ou un serveur, en utilisant les protocoles SSH, Telnet...etc. L'ensemble des sessions peuvent être automatiquement enregistrées sous forme de rapport afin d'être consultées ultérieurement.

Fortigate :

Fortigate est un des produits, dédié pour la sécurité réseau, fabriqué par l'entreprise Fortinet, leader dans la cyber sécurité et la protection contre les menaces. C'est un firewall de nouvelle génération avancé, autrement dit UTM, spécialement conçu pour la protection réseau en temps réel avec une approche de gestion unifiée des menaces.

Les équipements Fortigate Sécurisent les réseaux, réduisent les mauvais usages et abus réseaux et contribuent à une utilisation plus efficace des ressources de communication, sans compromettre la performance des communications réseau. La gamme a reçu les certifications ICSA[3] pare-feu, VPN IPSec et antivirus.

L'appliance FortiGate est entièrement dédié à la sécurité. Il est convivial et fournit une gamme complète de services de sécurité, que ce soit:

• Au niveau des applications (le filtrage antivirus, la protection contre les intrusions, les filtrages antispam, de contenu web et IM/P2P).

[3] ICSA est une certification qui donne l'assurance du niveau de sécurité du produit certifié, après une vérification stricte.

• Au niveau du réseau (le pare-feu, la détection et prévention d'intrusion, les VPN IPSec et VPN SSL et la qualité de service).

• Au niveau de l'administration (l'authentification d'un utilisateur, la journalisation et gestion des alertes, les profils d'administration, l'accès sécurisé au web et l'accès administratif CLI et SNMP).

Le système FortiGate utilise la technologie de Dynamic Threat Prevention System (Système Dynamique de Prévention des Attaques). Celle-ci s'appuie sur les dernières avancées technologiques en matière de conception de microcircuits, de gestion de réseaux, de sécurité et d'analyse de contenu. Cette architecture permet d'analyser en temps réel les contenus applicatifs et les comportements du réseau.

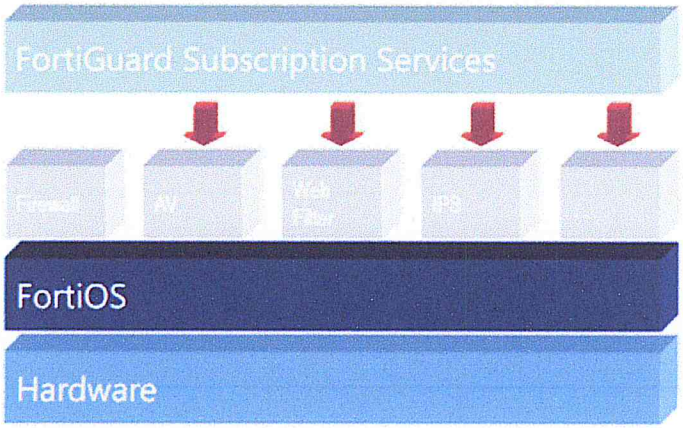


Figure 4.1: Design de la plateforme Fortigate

Dans le cadre de notre projet nous utilisons une image virtuelle Forigate dans sa dernière version à savoir version 5.6 éditée au mois d'avril 2018.

LOIC :

LOIC, pour Low Orbit Ion Cannon, qui peut être traduit par « canon à ion de basse orbite », il s'agit d'une application de test de réseau, écrite en C# et développée par Praetox Technologies. Cette application tente d'attaquer par déni de service la cible en l'inondant avec des paquets TCP, des paquets UDP, dont des requêtes HTTP avec l'intention de perturber le service d'un hôte particulier.

C'est une des sept outils d'attaque DOS les plus répandus. Elle a été utilisé particulièrement lors de trois attaques par le groupe hacktiviste Anonymous : l'Opération Chanology 3 du janvier 2008, quand les sites de l'Église de Scientologie ont été ciblés, l'Opération Payback 4

du septembre 2010, déclenchée contre les sites des organisations et des entreprises qui s'opposaient à WikiLeaks et l'Opération Megaupload 5 du janvier 2012, une forme de proteste à la fermeture du site de partage de fichiers Megaupload, décidé par le Département de la Justice des Etats-Unis. Cette dernière attaque a été, selon Anonymous, la plus grande attaque par déni-de-service sur Internet.

4. Mise en œuvre de la solution :

Cette section aborde la simulation de la mise en œuvre de la solution spécifiée au chapitre précèdent, avec ses deux volets. Pour cela nous commençons par mettre en place l'architecture de déploiement grâce à l'émulateur EVE NG, ensuite nous passons au déploiement du firewall Fortigate au niveau du réseau.

4.1Mise en place de l'architecture de déploiement :

Après l'installation des outils nécessaires, vient la création de la topologie de test en se basant sur l'architecture de sécurité proposée pour l'extranet. Quant à l'intranet nous prenons une des agences comme exemple, et ça sera exactement la même démarche pour le reste des sites de la CNEP banque.

La figure 4.2 représente la topologie de déploiement sur laquelle la solution est testée.

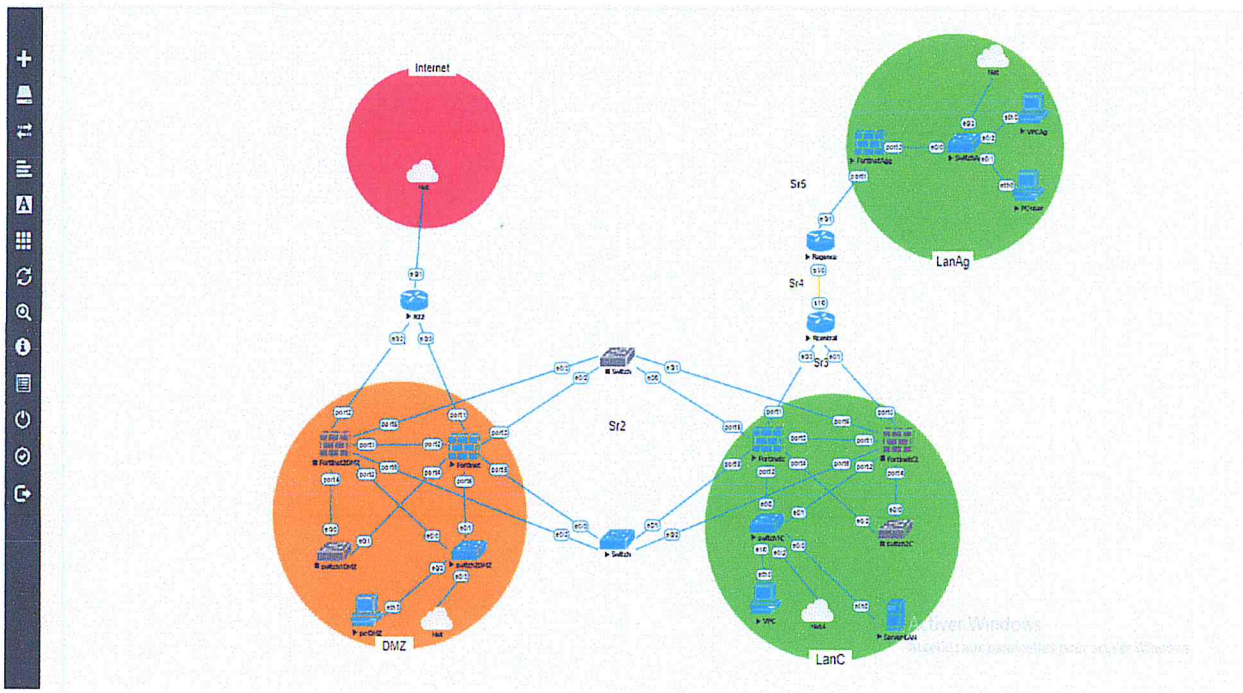


Figure 4.2 : Topologie de déploiement

La convention de nommage correspondant à la topologie de déploiement est présentée dans **le tableau 4.1**.

Périphériques	Description
Rinternet	Routeur d'accès à Internet
Rcentral	Routeur du site central
Ragence	Routeur de l'agence test
Switch1DMZ	Switch d'accès à la DMZ du site central
Switch2DMZ	Switch d'accès à la DMZ du site central
SwitchC1	Switch d'accès au LAN du site central
SwitchC2	Switch d'accès au LAN du site central
FortinetDMZ1	Firewall de protection de la DMZ
FortinetDMZ2	Firewall de protection de la DMZ
Fortinet1C	Firewall de protection du LAN du site central
Fortinet2C	Firewall de protection du LAN du site central
FortinetAg	Firewall de protection de l'agence test
PC-user	Hôte final de l'agence de test
PC-LAN	Hôte final de l'agence de test

Tableau 4.1: Convention de nommage des équipements

Afin d'assurer une connectivité réseau de bout en bout, nous effectuons une configuration de base pour notre laboratoire. À commencer par l'adressage des nœuds, ensuite la définition des routes. Quant à l'adressage des hôtes finaux, nous procédons à un adressage statique, les sous réseaux sont présentés dans le **tableau 4.2**.

Le choix du mode de routage est important, nous optons pour un routage statique, il est plus adapté à nos besoins. En effet, le routage statique présente plusieurs avantages :

- **Sécurité** : Contrairement aux protocoles de routage dynamique, le routage statique ne diffuse pas d'information sur le réseau puisque les informations de routage sont directement saisies dans la configuration des routes.
- Économie de bande passante : Étant donné qu'aucune information ne transite entre les routeurs pour qu'ils se tiennent à jour, la bande passante n'est pas encombrée avec des messages d'information et de routage.

- Connaissance du chemin à l'avance : en ayant configuré l'ensemble de la topologie nous savons exactement par où passent les paquets pour aller d'un réseau à un autre, cela peut donc faciliter la compréhension d'un incident sur le réseau lors des transmissions de paquets.

Attribution	Adresse sous réseau	Diffusion	Passerelle
Sr1	192.168.11.0/24	192.168.11.255	192.168.11.1
Sr2	192.168.12.0/24	192.168.12.255	192.168.12.1
Sr3	192.168.13.0/24	192.168.13.255	192.168.13.1
Sr4	192.168.14.0/24	192.168.14.255	192.168.14.1
Sr5	192.168.15.0/24	192.168.15.255	192.168.15.1
LAN-Ag	192.168.16.0/24	192.168.16.255	192.168.16.1
LAN-C	192.168.17.0/24	192.168.17.255	192.168.17.1
DMZ	192.168.18.0/24	192.168.18.255	192.168.18.1
Internet	192.168.8.0/24	192.168.8.255	192.168.8.1

Tableau 4.2 : Sous-réseaux correspondants à la topologie de déploiement

4.2 Déploiement du Fortigate :

Après son installation au niveau du réseau, le Fortigate requiert une configuration de base pour son système, pour assurer une bonne communication avec le reste des équipements réseau et garantir l'accès sécurisé à l'équipement, ainsi nous procédons à la mise en place des mesures de sécurité.

4.2.1 Configuration système :

Le réglage initial du dispositif Fortigte nécessite une connexion depuis la CLI, avec le nom d'utilisateur par défaut « admin », et sans mot de passe.

- Configuration du nom système de l'équipement Fortigate :

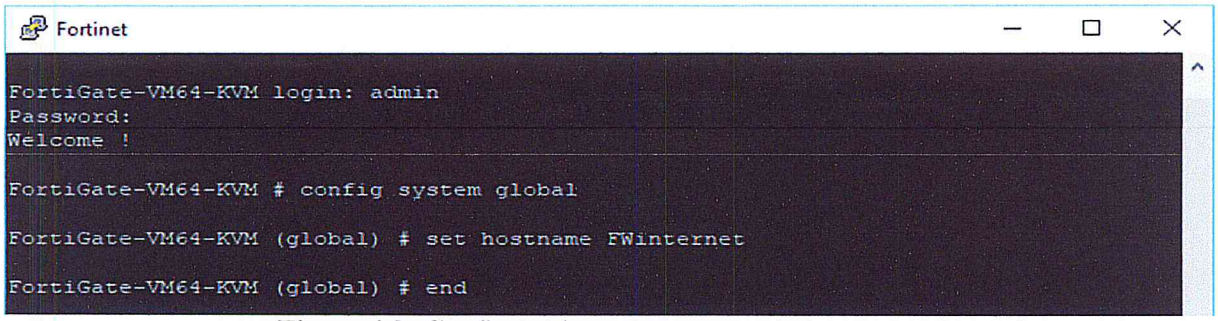


Figure 4.3: Configuration du Hostname du Fortigate

- Configuration du temps d'administration par défaut :

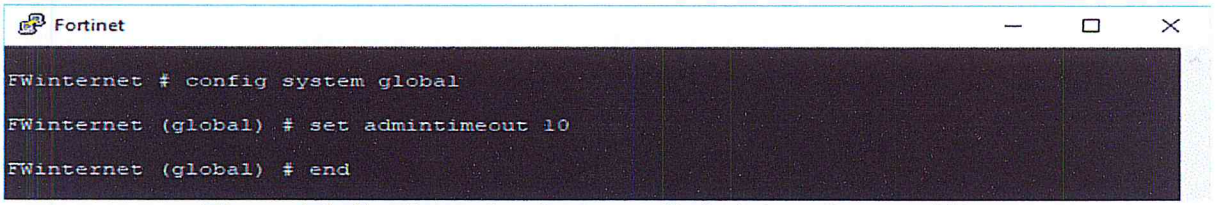


Figure 4.4: Configuration du temps d'administration par défaut

- Configuration de l'adresse IP du port1 et activation des protocoles d'administration sur le même port:

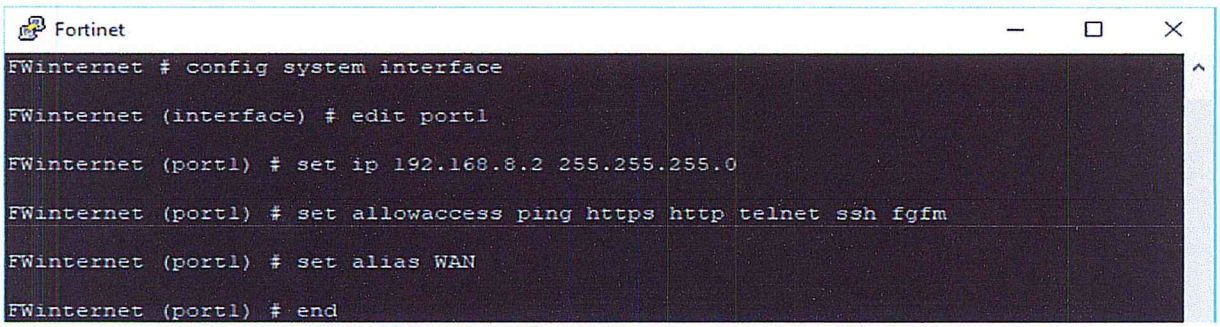


Figure 4.5: Adressage et configuration des protocoles d'administration

- Configuration de la route par défaut :

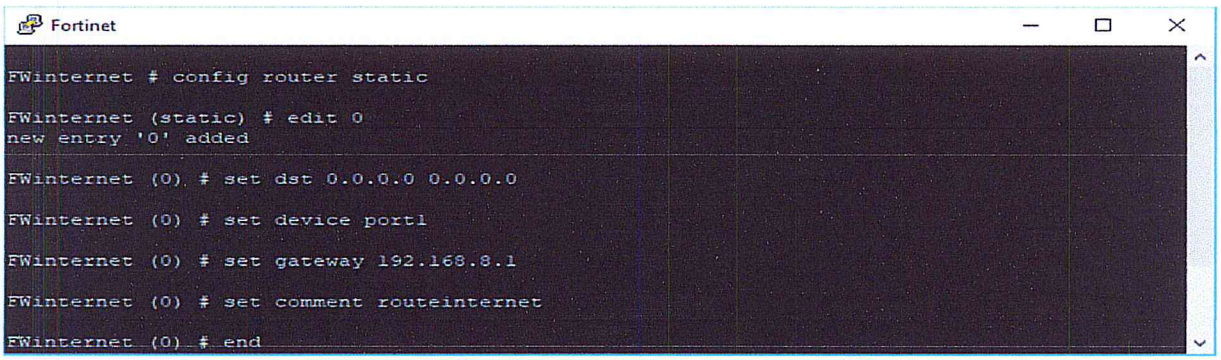


Figure 4.6: Configuration de la route par défaut

L'accès à la WUI devient possible, en entrant l'adresse IP du port1 au navigateur web, suivi des paramètres d'authentification par défaut, pour ainsi poursuivre la configuration initiale à partir de la WUI :

- Changement des paramètres d'authentification par défaut du firewall :

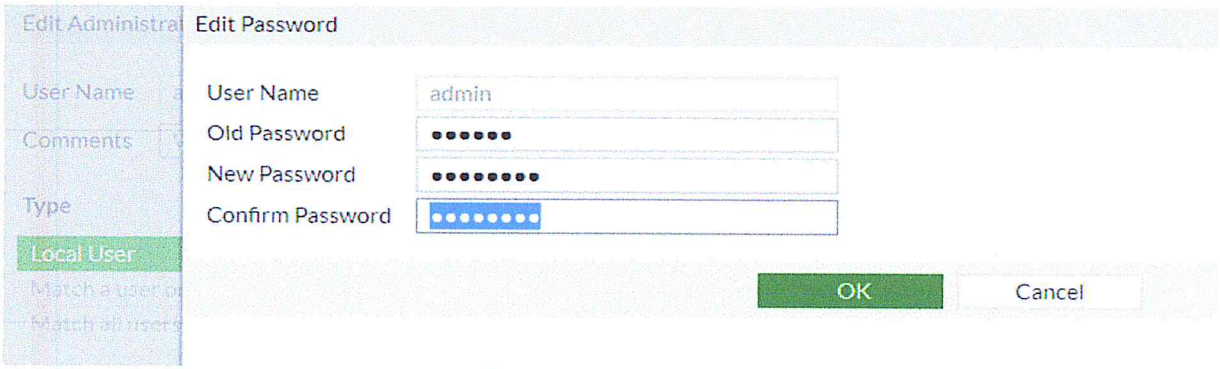


Figure 4.7: Modification des paramètres d'authentification du firewall

- Configuration du fuseau horaire du firewall selon notre zone géographique :

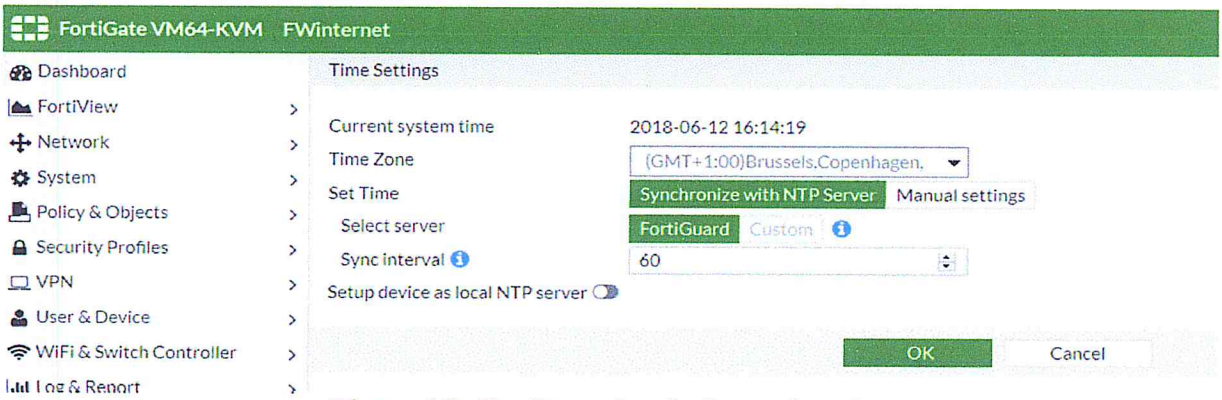


Figure 4.8: Configuration du fuseau horaire

4.2.3 Mise en place des mesures de sécurité :

Afin de permettre une meilleure structuration de la mise en place des mesures de sécurité, nous l'avons divisé en plusieurs étapes, suivi des tests et résultats.

a. Gestion des accès LAN et WAN :

Il s'agit de la définition des règles de contrôle d'accès entre les différents sites. Cette fonction permet d'éliminer tout trafic inutile ou suspect, et aussi de diminuer la charge sur les liaisons.

Pour l'agence, l'accès n'est autorisé qu'au réseau local du site principal, les règles de contrôle d'accès établies sont représentées par la matrice de trafic suivante :

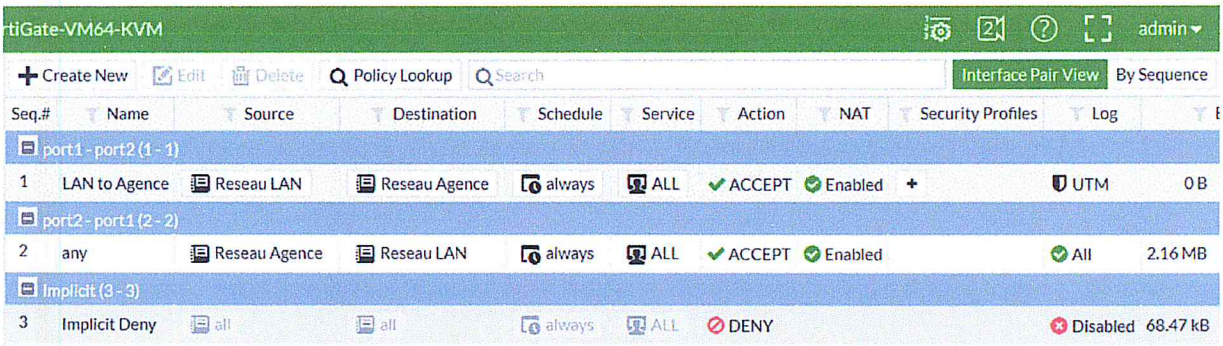


Figure 4.9: Matrice de contrôle d'accès au niveau de l'agence

La configuration d'une règle de sécurité pour le contrôle d'accès sur Fortigate se fait en tous les éléments nécessaires :

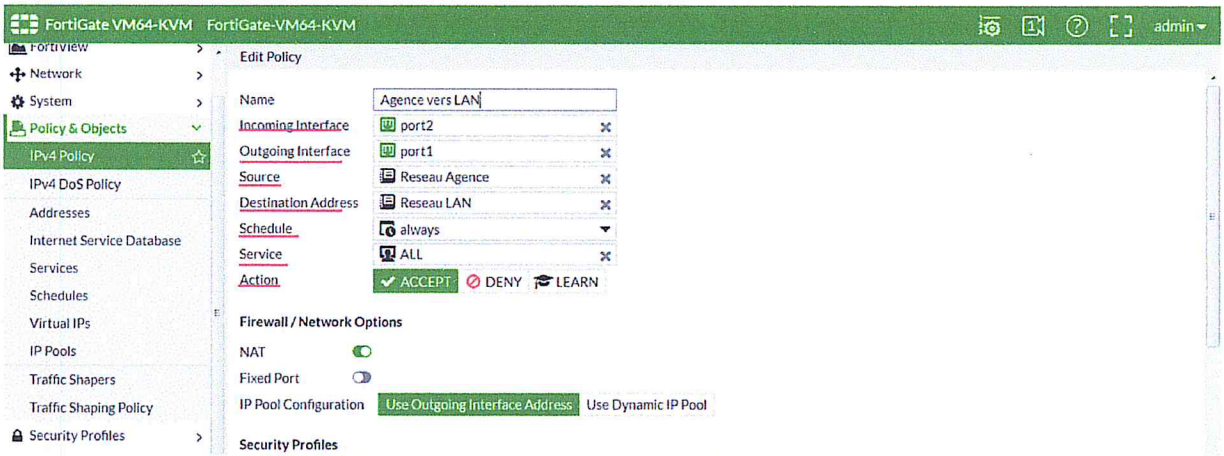


Figure 4.10: Exemple de configuration d'une règle de contrôle d'accès Fortigate

En effectuant un test de Ping, depuis l'agence vers le site principal, la DMZ et internet, **voir la Figure 4.11.**

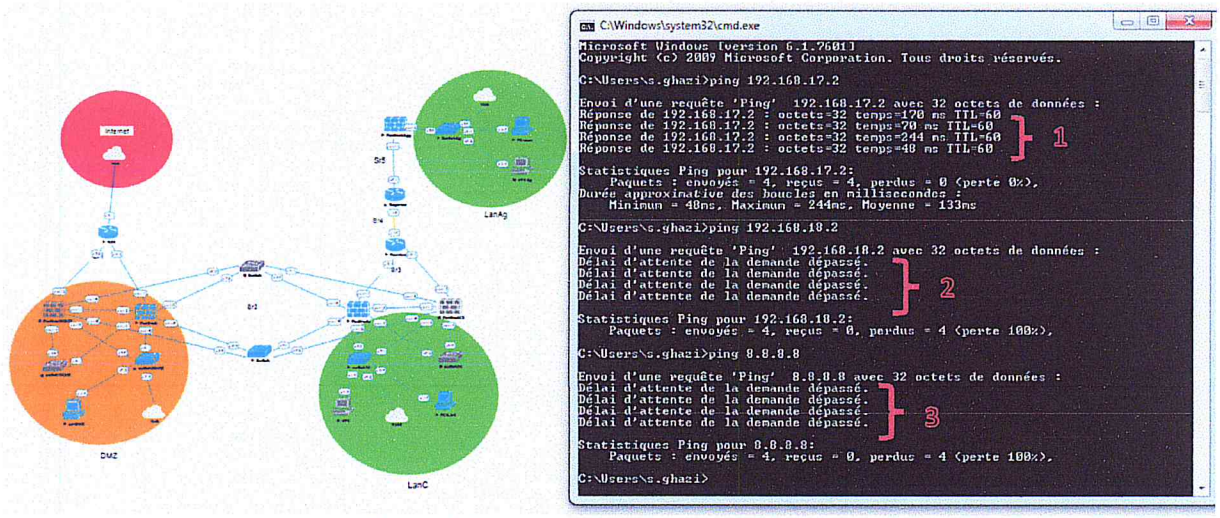


Figure 4.11: Test d'accès depuis l'agence

Nous obtenons ce qui suit :

(1) L'accès au site principal est autorisé.

(2) L'accès à la DMZ est refusé.

(3) L'accès à internet est refusé.

Pour le site principal, l'accès est autorisé vers l'agence, la DMZ, et internet, les règles de contrôle d'accès établies sont représentées par la matrice de trafic suivante :

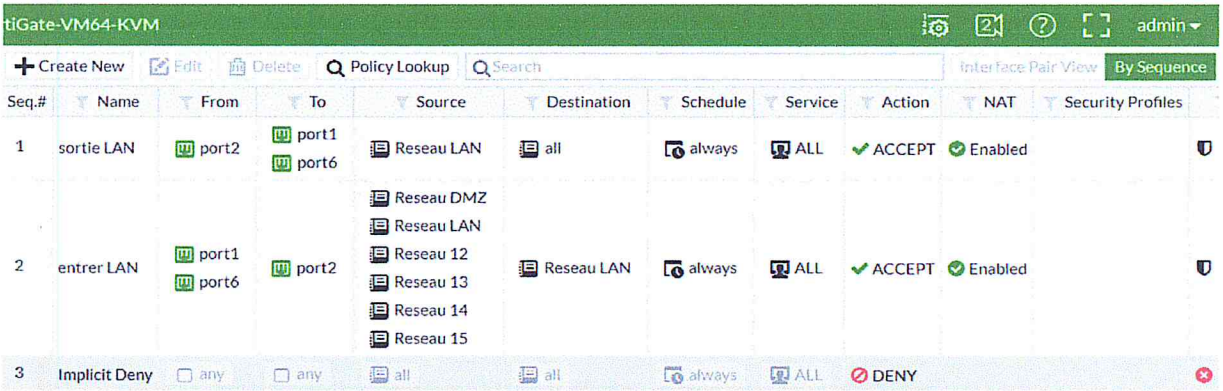


Figure 4.12: Matrice de contrôle d'accès au niveau du site principal

En effectuant un test de Ping, depuis le site principal, vers internet, DMZ et Agence, **voir la Figure.**

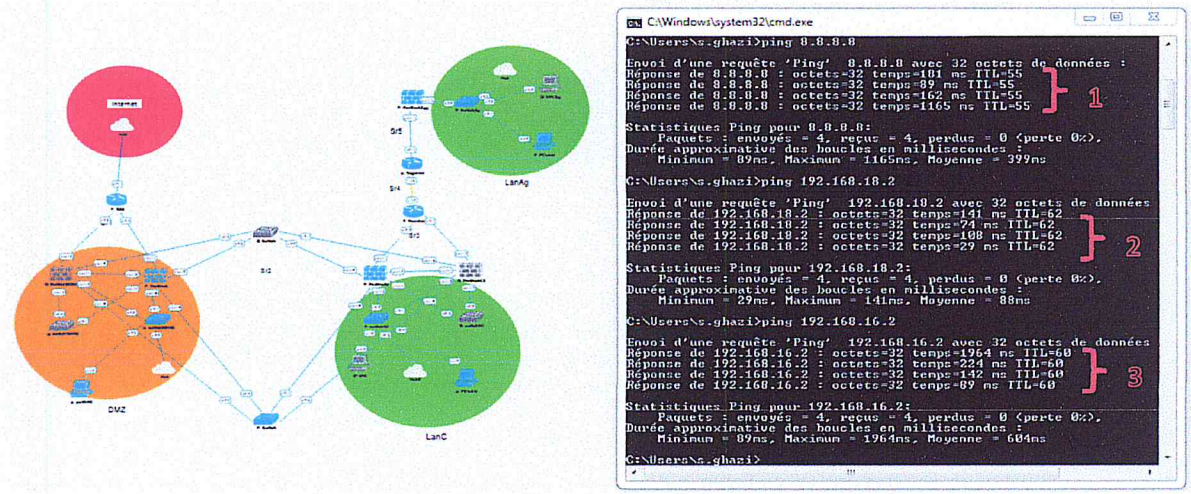


Figure 4.13: Test d'accès depuis le site principal

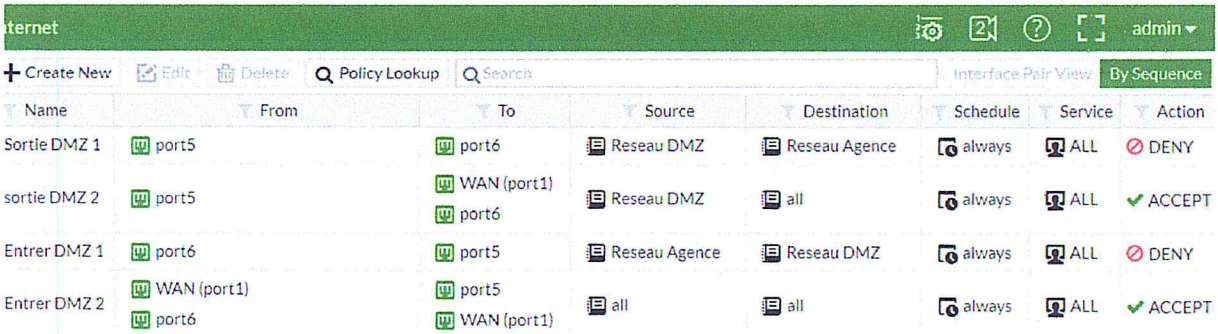
Nous obtenons ce qui suit :

(1) L'accès à internet est autorisé.

(2) L'accès à la DMZ est autorisé.

(3) L'accès à l'agence est autorisé.

Pour la DMZ, l'accès n'est autorisé que vers le site principal et internet, les règles de contrôle d'accès sont représentées par la matrice de trafic suivante :



Name	From	To	Source	Destination	Schedule	Service	Action
Sortie DMZ 1	port5	port6	Reseau DMZ	Reseau Agence	always	ALL	DENY
sortie DMZ 2	port5	WAN (port1) port6	Reseau DMZ	all	always	ALL	ACCEPT
Entrer DMZ 1	port6	port5	Reseau Agence	Reseau DMZ	always	ALL	DENY
Entrer DMZ 2	WAN (port1) port6	port5 WAN (port1)	all	all	always	ALL	ACCEPT

Figure 4.14: Matrice de contrôle d'accès au niveau de la DMZ

En effectuant un test de Ping, depuis la DMZ vers internet, vers le site principal et l'agence nous obtenons :

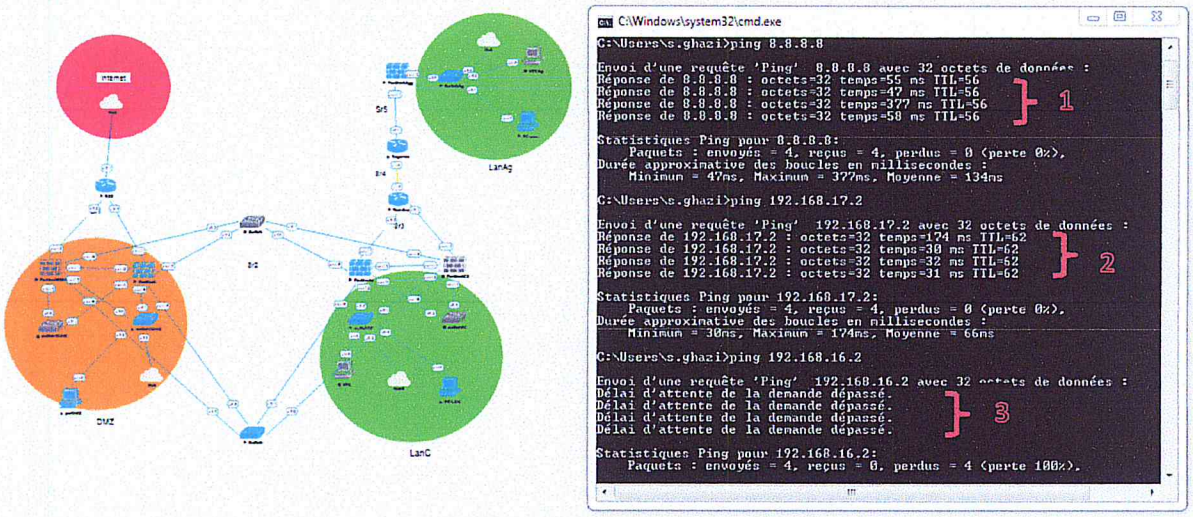


Figure 4.15: Test d'accès depuis la DMZ

(1) L'accès à internet est autorisé.

(2) L'accès au site principal est autorisé.

(3) L'accès à l'agence est refusé.

b. Gestion de la bande passante :

Il s'agit d'allouer une bande passante pour chaque trafic. Afin de prioriser un trafic par rapport à un autre sur une même liaison, selon les critères définies.

Sa configuration passe par la spécification du type de trafic à gérer sa priorité ainsi que le maximum et le minimum de bande passante allouée, comme l'illustre **la figure 4.16**.

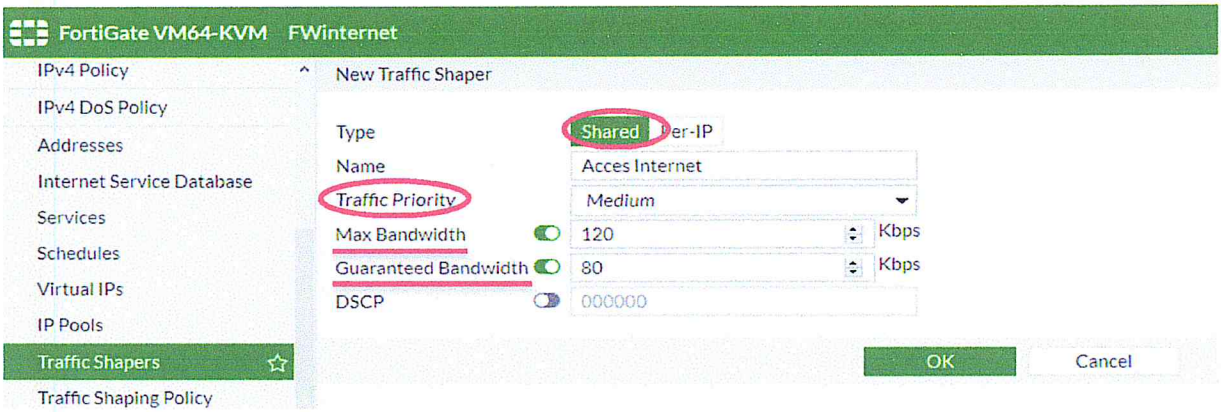


Figure 4.16: Spécification de la bande passante

Ensuite l'application du profil spécifié, sur le flux correspondant, **voir la figure 4.17**.

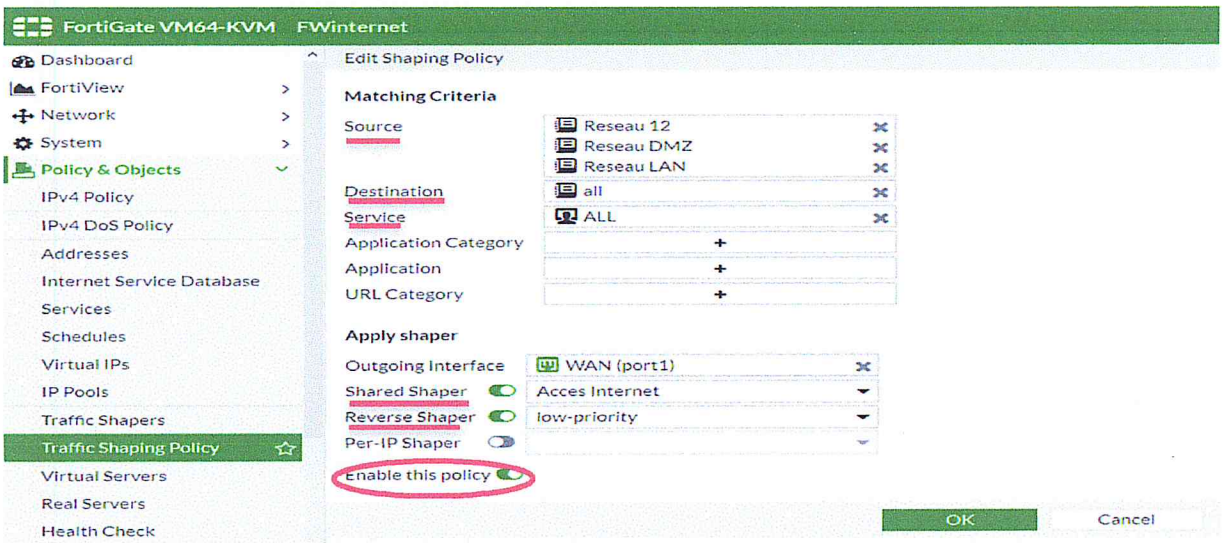


Figure 4.17: Création de la règle de gestion de la bande passante

Après la configuration de plusieurs règles, la matrice des règles de gestion de bandes passantes apparaît comme sur **la figure 4.18**.

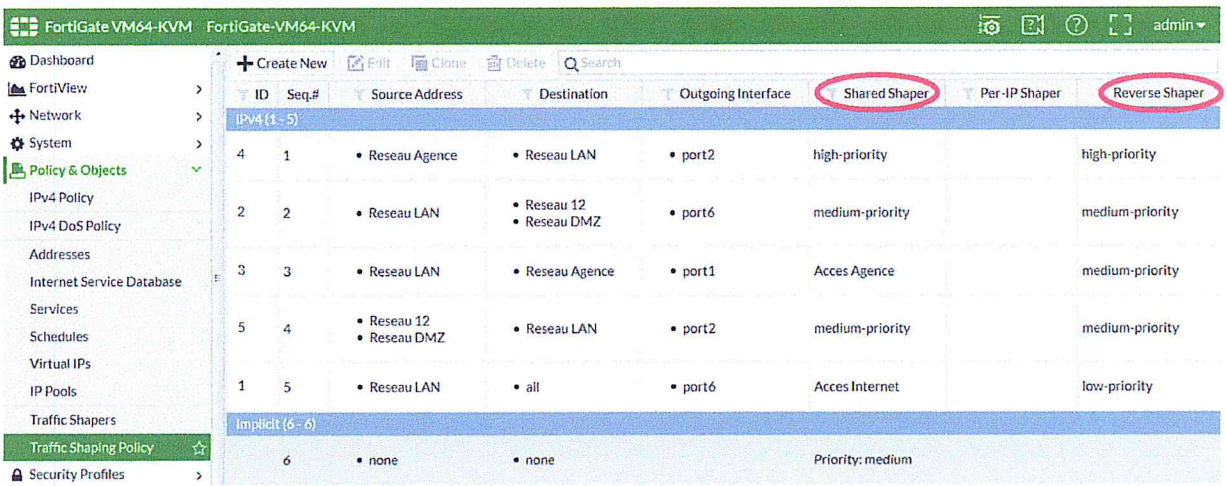


Figure 4.18: Matrice des règles de gestion de la bande passante du site principal

c. Analyse antivirale :

Il s'agit de l'activation de l'analyse antivirale, elle permet la détection et l'élimination des logiciels malveillants embarqués dans les paquets qui transitent le réseau, les APTs ou tout autre code informatique suspect.

i. Configuration :

La protection des logiciels malveillants déjà connu nécessite la création d'un profil de sécurité et spécifier les protocoles concernés par l'inspection comme l'illustre **la figure 4.19,** ensuite appliquer le profil crée sur les règles de sécurité définies, voir **la figure4.34**.

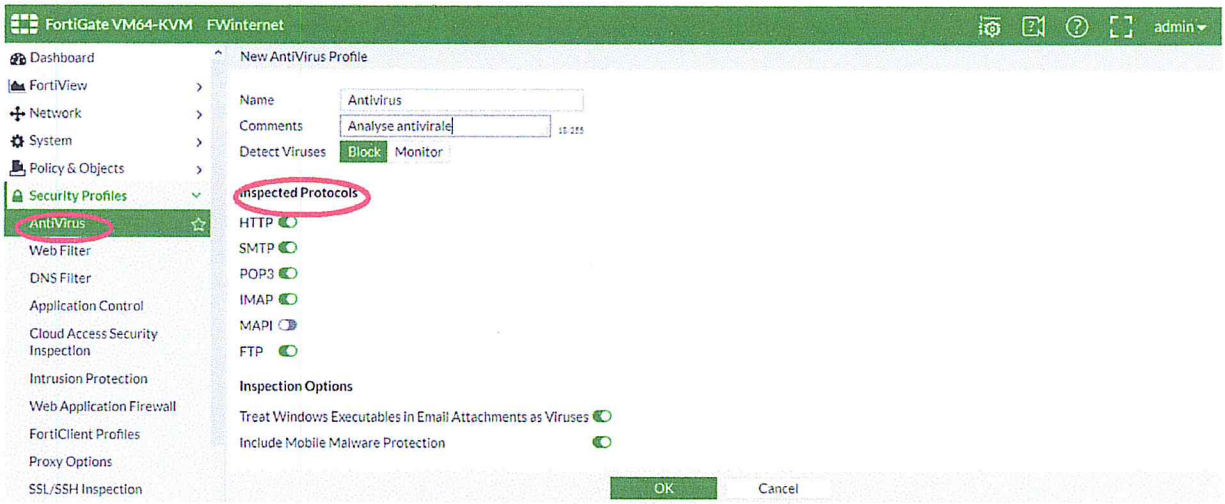


Figure 4.19: Création d'un profil Antiviral

La protection contre les gryware[4] ainsi que l'analyse antivirale heuristique pour la protection contre les APT, nécessite une activation depuis la CLI, voir **la figure4.20**.

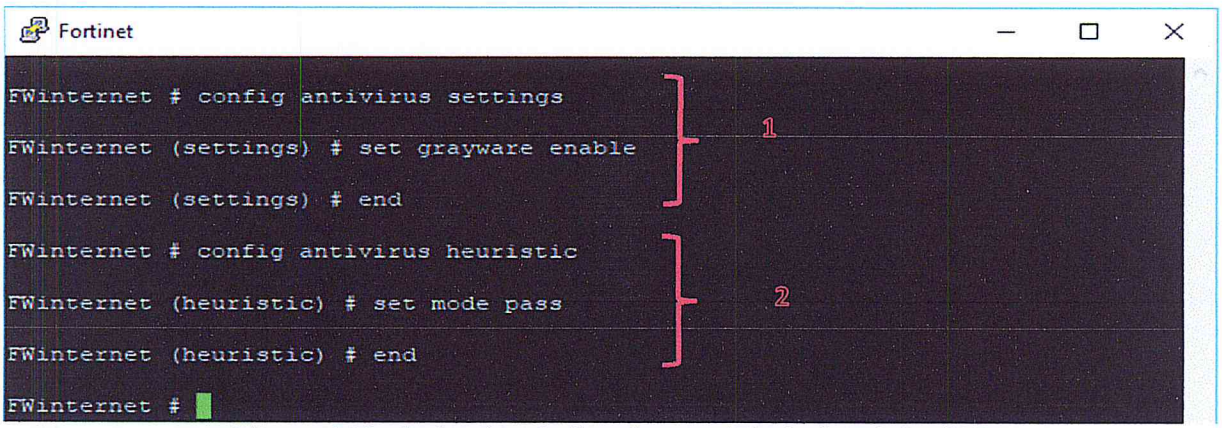


Figure 4.20: Activation de l'analyse antivirale depuis la CLI

[4] Désignent des applications ou des fichiers qui ne sont pas classés comme virus ou chevaux de Troie, mais qui peuvent néanmoins endommager la performance des ordinateurs du réseau.

(1) Activation de la protection contre les grayware.

(2) Activation de l'analyse antivirus heuristique.

Vu le taux de faux positif qui peut être généré dans le cas où nous bloquons tout code informatique suspect grâce à l'analyse heuristique, nous préférons plutôt les gérer au niveau de l'intranet, en activant le mode « Pass ». Ainsi les paquets concernés peuvent passer mais ils seront signalés. Quant à l'extranet nous préférons les bloquer, nous pensons qu'il est plus probable qu'une attaque aussi sophistiquée provient de l'extérieur que de l'intérieur du réseau.

ii. Test :

Pour l'évaluation du fonctionnement de l'analyse antivirale, il suffit d'accéder à www.eicar.org et essayer de télécharger le fichier eicar.com[5]. **La figure4.21** montre que le fichier est bloqué par l'antivirus.

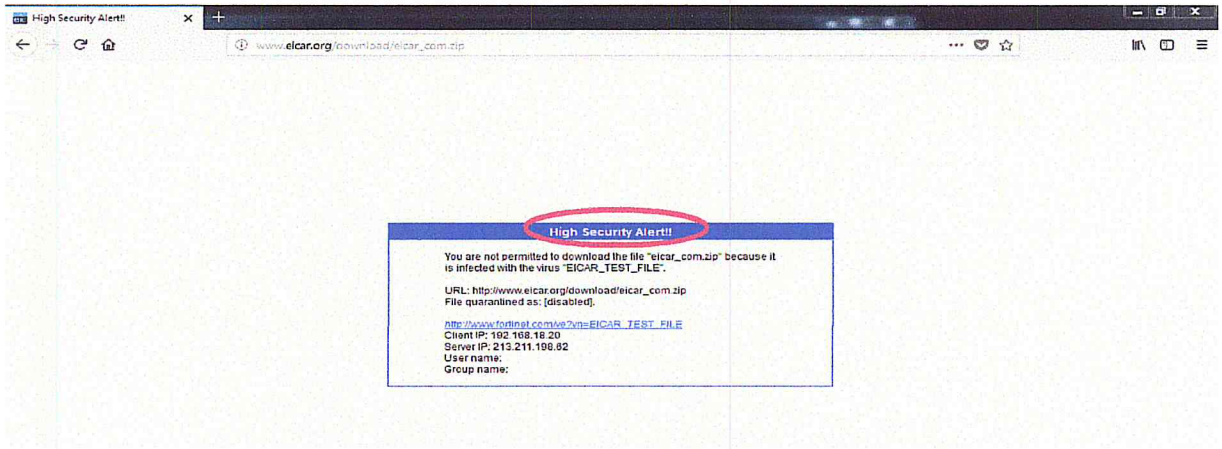


Figure 4.21: Résultat du test de l'analyse antivirale

d. Filtrage web :

Il s'agit de contrôler les accès web en autorisant, bloquant ou limitant certains sites. Cette fonction permet de bloquer les sites suspects, malveillants et gourmands en bande passante et garantir l'accès aux sites liés à l'activité financière et bancaire ou portail gouvernementaux.

i. Configuration :

Il est possible d'effectuer un filtrage web statique, par URL simple ou en définissant des modèles d'URLs avec des expressions régulières, voir **la figure4.22**.

[5] Le fichier de **test Eicar** est une chaîne de caractères, écrite dans un fichier informatique, destiné à tester le bon fonctionnement des logiciels antivirus. En anglais, il est dénommé « **Anti-Virus test file** ».

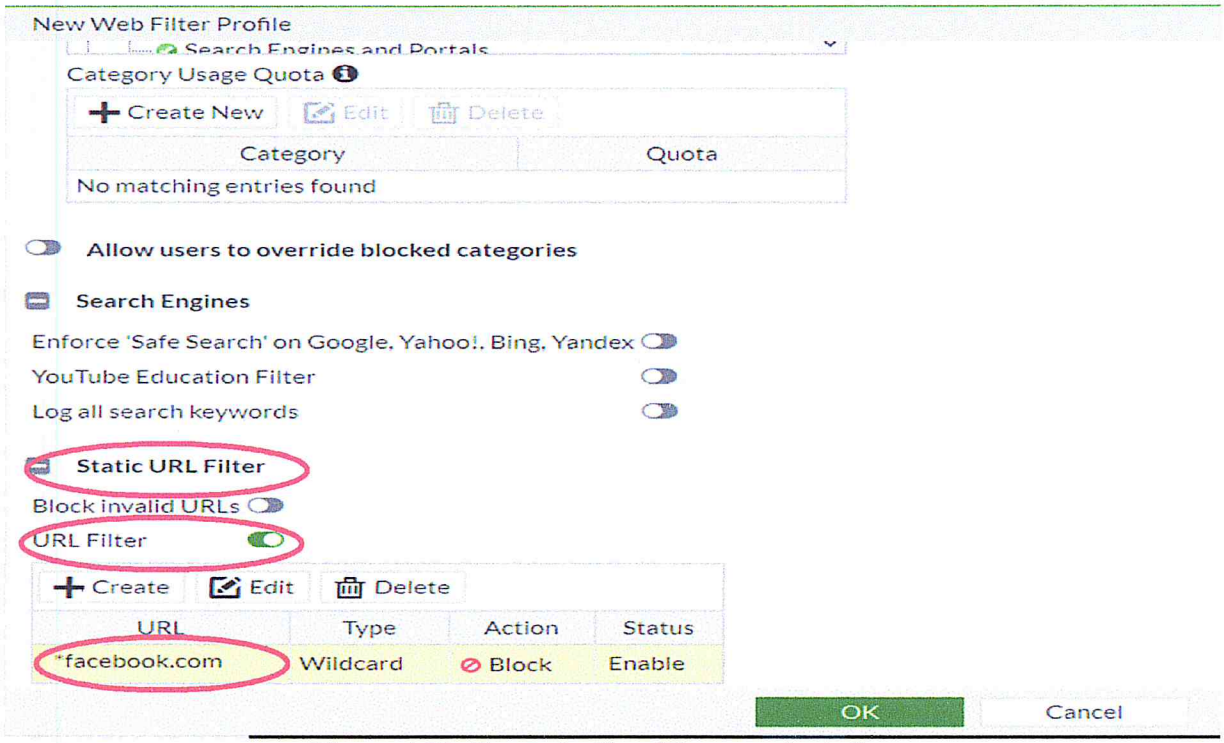


Figure 4.22: Exemple d'un filtrage web statique

Nous préférons d'activer le filtrage par catégorie vu que la catégorisation Fortigate est assez exhaustive et elle change périodiquement selon l'évolution de l'internet, de plus elle est moins onéreuse. Voir **la Figure4.23.**

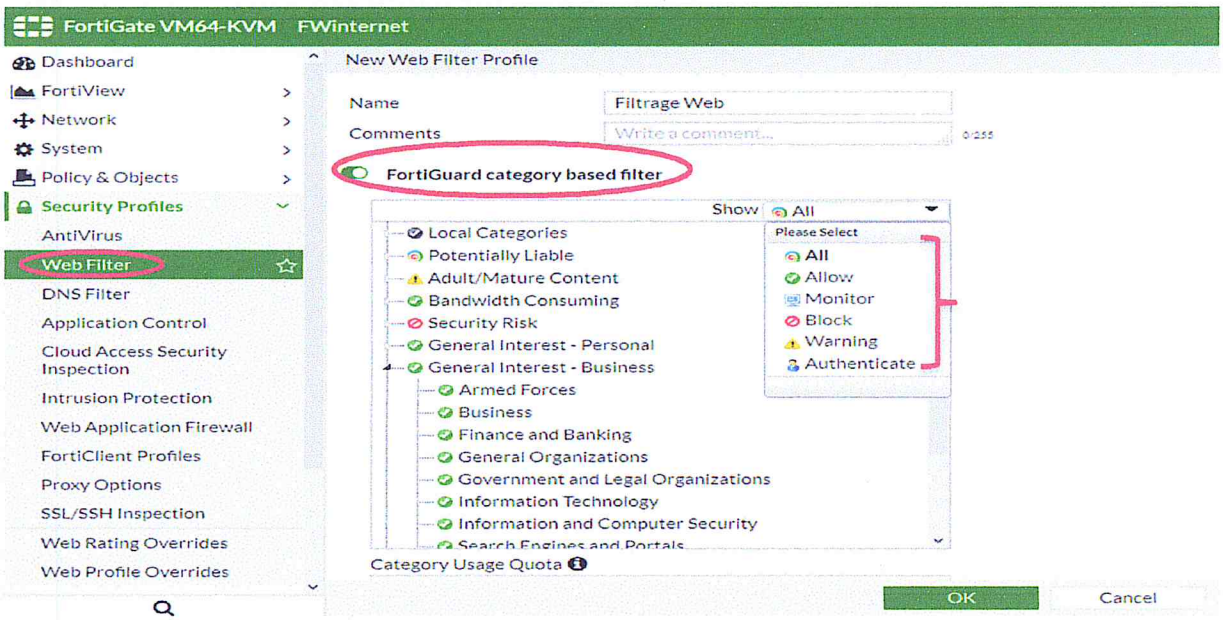


Figure 4.23: Création d'un profil de filtrage web

ii. Test :

Afin de tester le fonctionnement du filtrage web établit, nous essayons en premier lieu d'accéder à un site web malveillant à l'exemple du site de hacking www.serial.ws .

Sur **la figure 4.24**, nous pouvons apercevoir que le site web est bloqué.

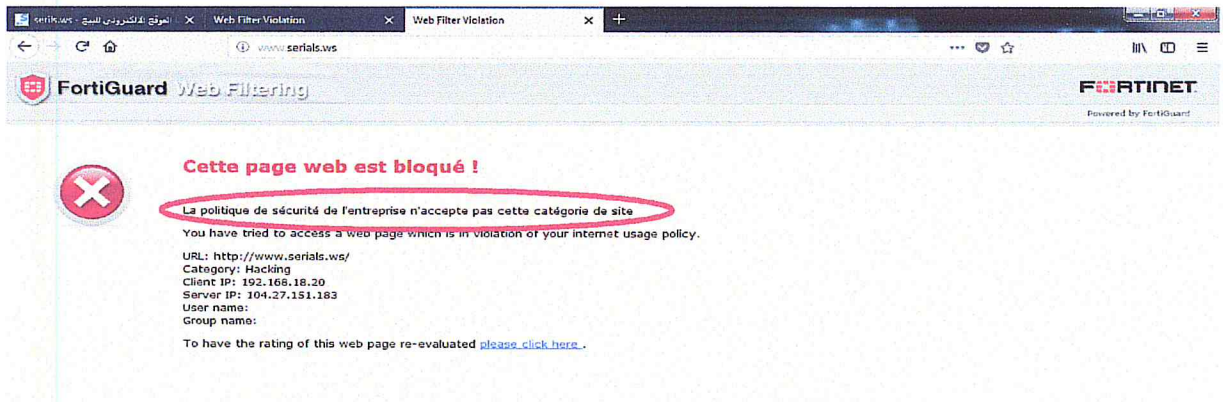


Figure 4.24: Filtrage web d'un site malveillant

En second lieu, nous essayons d'accéder aux sites autorisés mais avec un avertissement indiquant à l'utilisateur que tout risque provenant du site est sous sa responsabilité. C'est le cas des réseaux sociaux qui véhicule un grand nombre de menaces, à l'exemple de www.facebook.com , voir **la figure4.25**.

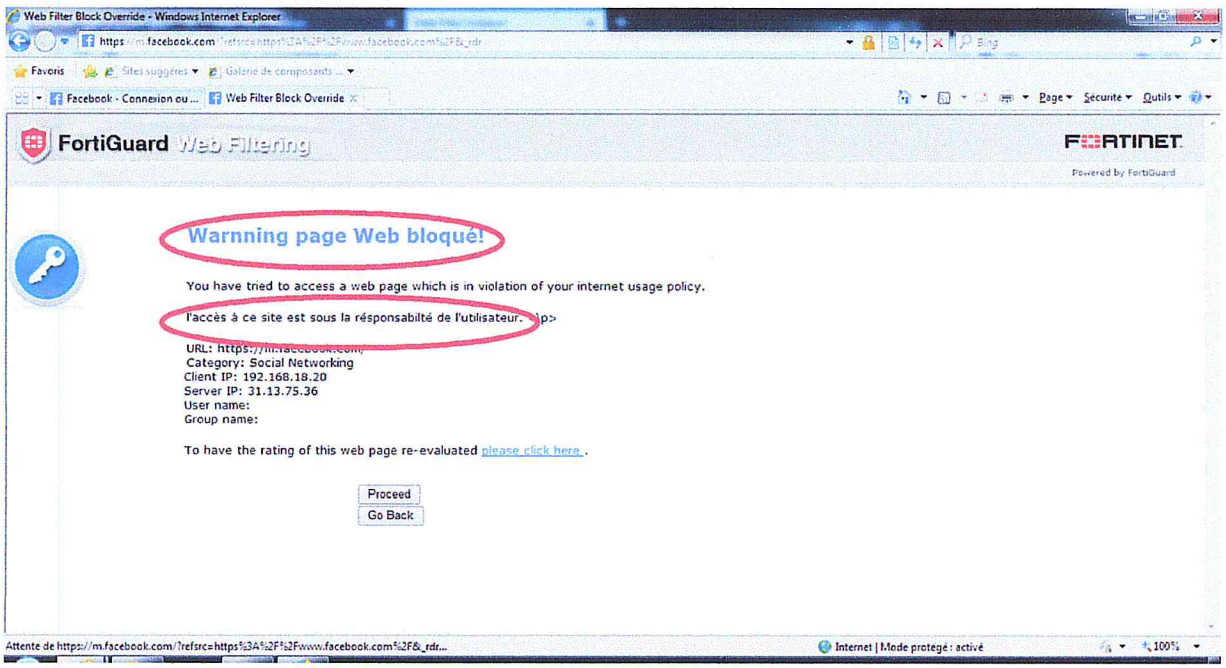


Figure 4.25: filtrage web d'un site autorisé avec avertissement

En troisième lieu, pour s'assurer que l'accès aux sites autorisés est encore possible, nous essayons un certain nombre sites, à l'exemple de www.ebank.cnepbanque.dz . Voir **la figure4.26**.

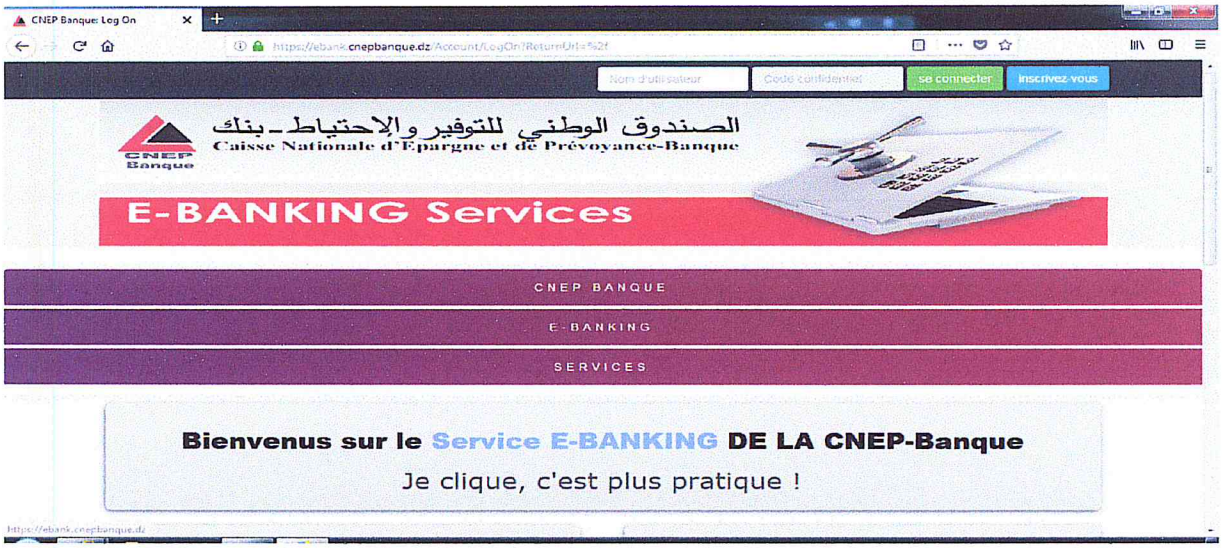


Figure 4.26: Accès à un site autorisé

Enfin, nous essayons d'accéder en utilisant un logiciel proxy à l'exemple de « Tor ». L'accès est autorisé, voir **la figure4.27.**

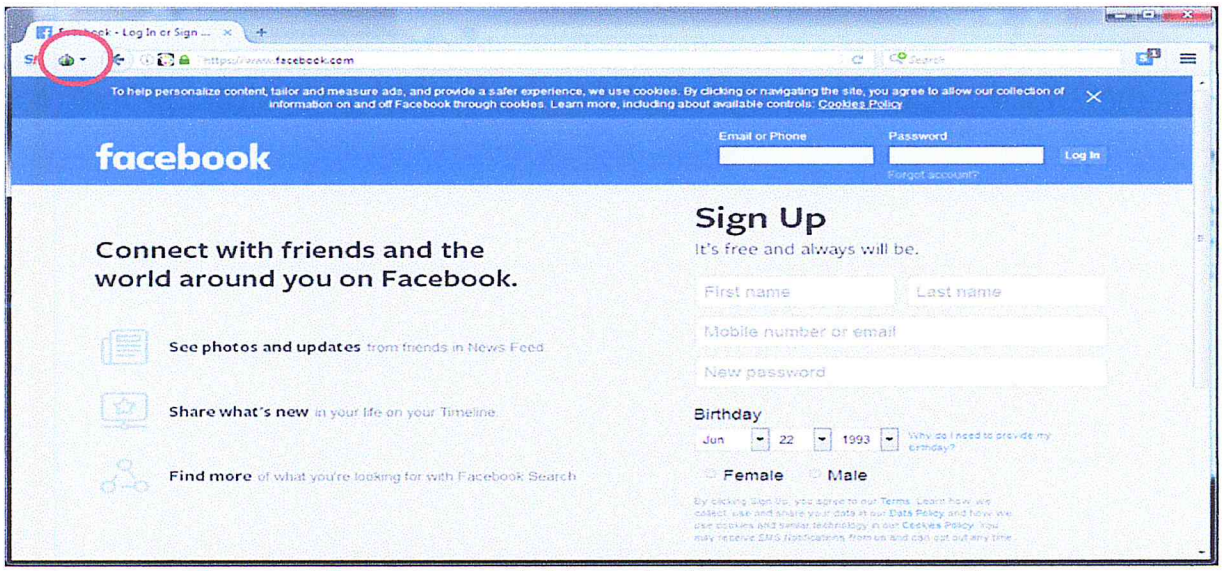


Figure 4.27: Accès autorisé à un site bloqué, depuis un « Tor »

D'après les résultats obtenus, nous constatons qu'il est possible de contourner les règles de sécurité établies via un proxy externe, il convient de bloquer l'accès aux applications de type proxy et effectuer un contrôle applicatif pour le reste des applications.

e. Contrôle applicatif :

Il s'agit de détecter et agir sur le trafic des applications en réseau. Ceci permet de bloquer les applications malveillantes, suspects, gourmande en bande passante et gérer le trafic de celles qui ne sont pas liées à l'activité de l'entreprise ou encore celles permettant de contourner les règles de sécurité établies.

i. Configuration :

La configuration du contrôle applicatif consiste d'abord à créer le profil souhaité et spécifier l'action à appliquer pour chacune des catégories d'application voir **la figure4.28**, ensuite appliquer le profil crée sur les règles de sécurité définies voir **la figure4.34**. Il est également possible d'ajouter de nouvelles signatures d'applications.

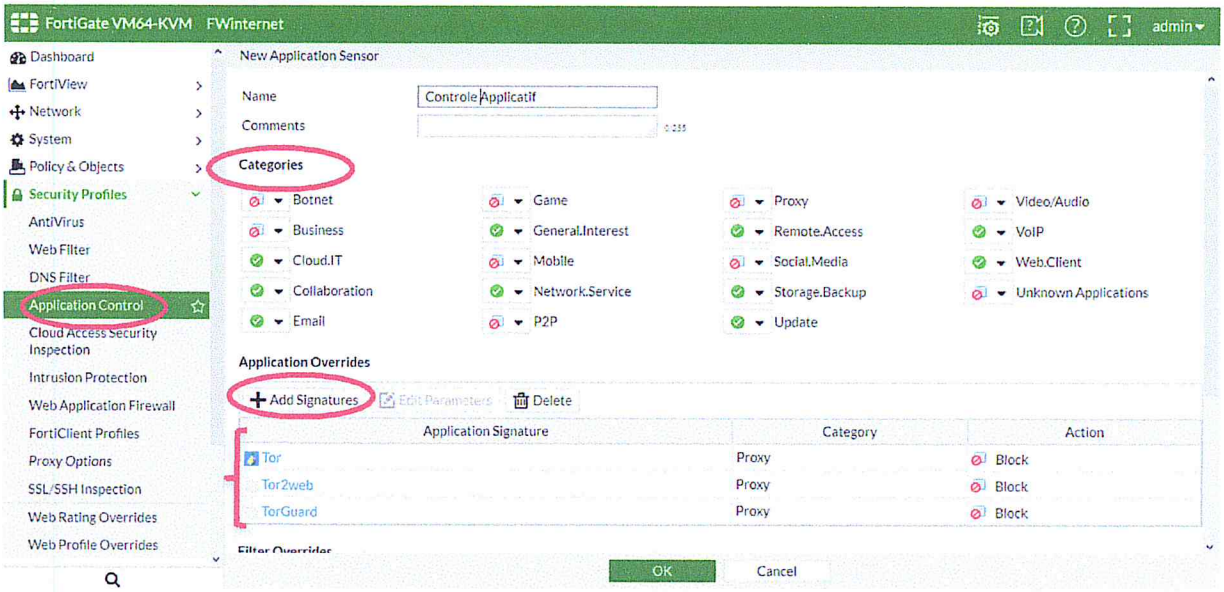


Figure 4.27: Création d'un profil de control applicatif

(1) Catégories Autorisées et refusée.

(2) Signatures d'application rajoutées.

Les signatures sont ajoutées par catégorie et risque, comme l'illustre **la figure4.28**.

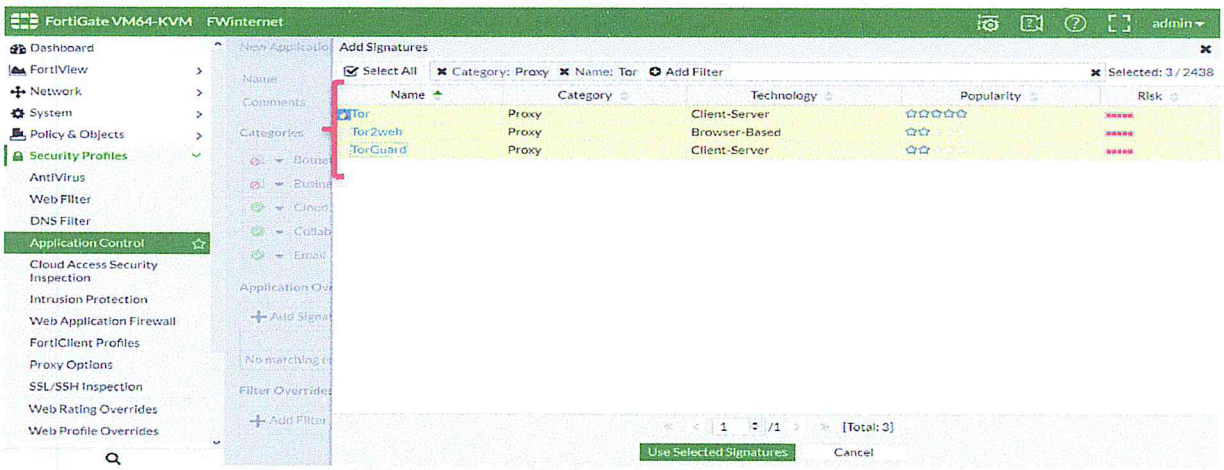


Figure 4.28: Exemple d'ajout de signatures d'application

ii. Test :

Afin de tester le fonctionnement du contrôle applicatif, nous essayons de se connecter à internet en utilisant l'application « Tor », **voir la figure4.29.**

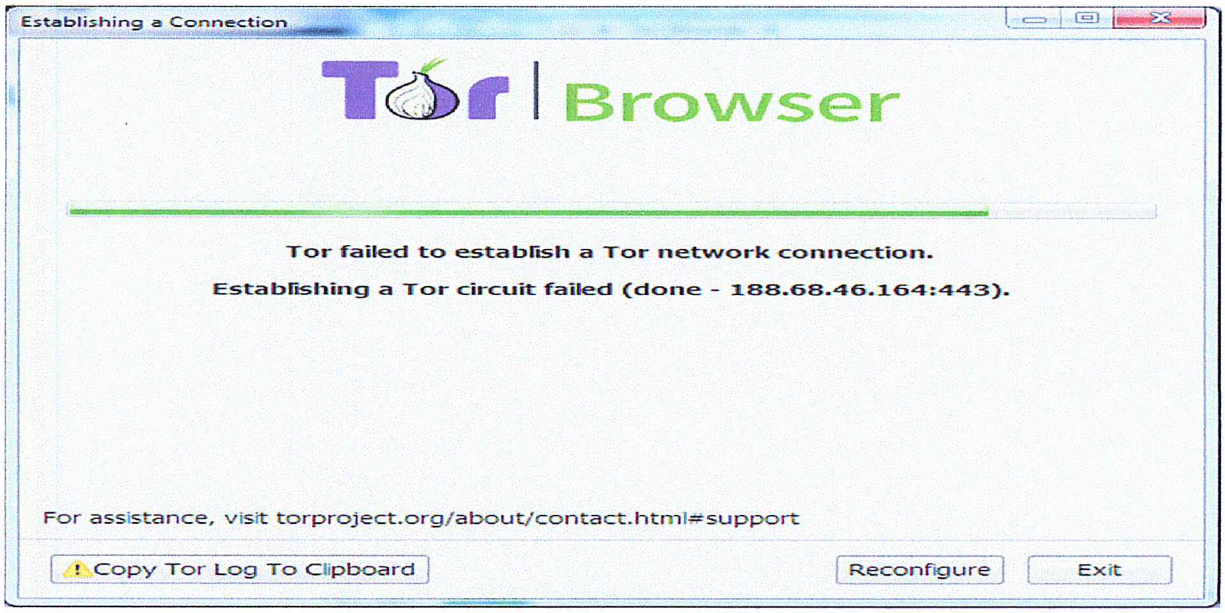


Figure 4.29: Blocage de l'application TOR

D'après **la figure4.29**, nous constatons que l'accès à l'application est refusé ce qui montre l'efficacité du contrôle applicatif établit.

f. Prévention d'intrusion :

La configuration de l'ips commence par la création d'un profil de prévention d'intrusion.

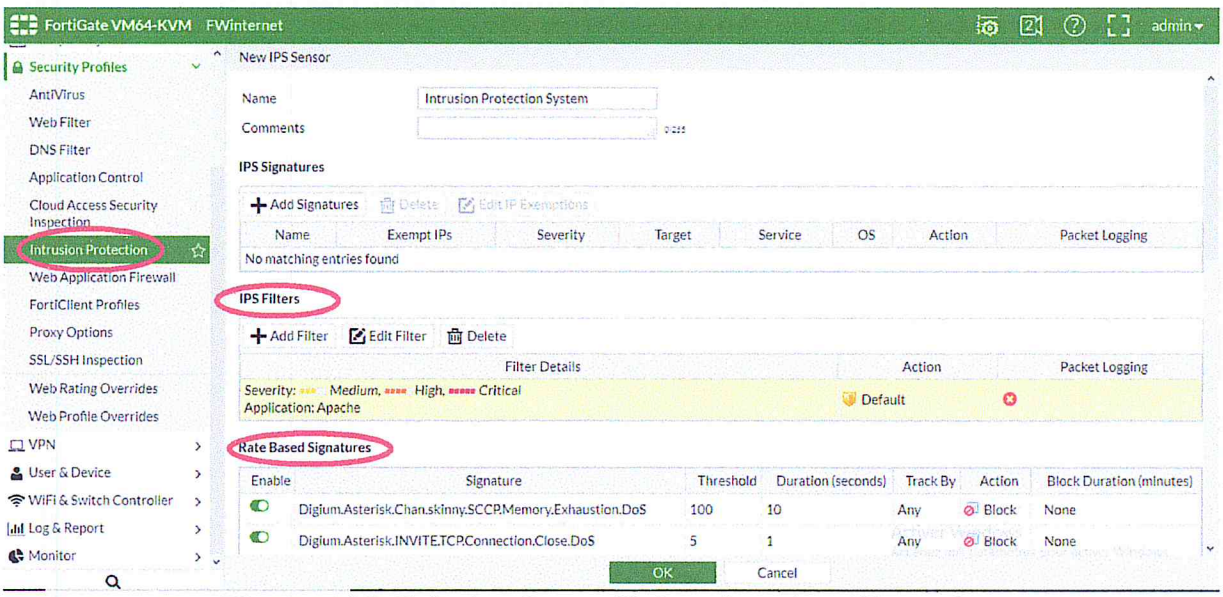


Figure 4.30:Création du profil de prévention d'intrusion

Ensuite choisir les signatures à bloquer depuis la base de données par degré de sévérité, comme le montre **la figure4.31**.

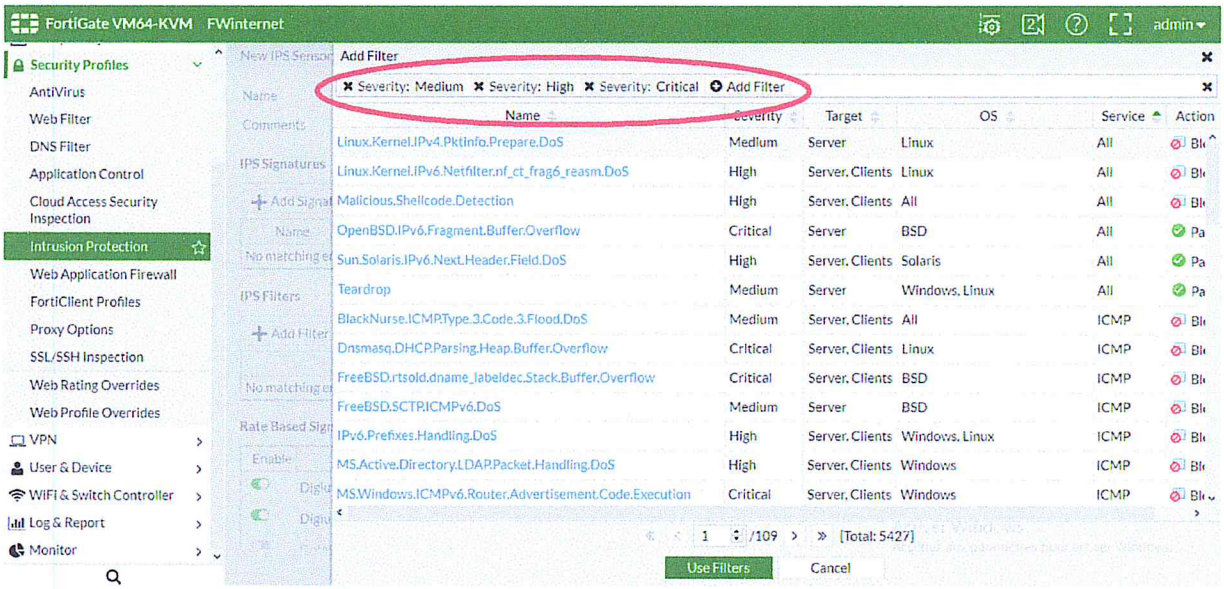


Figure 4.31: Sélection des signatures IPS

Il est possible également d'ajouter de nouvelles signatures, comme le montre l'exemple de **la figure 4.32.**

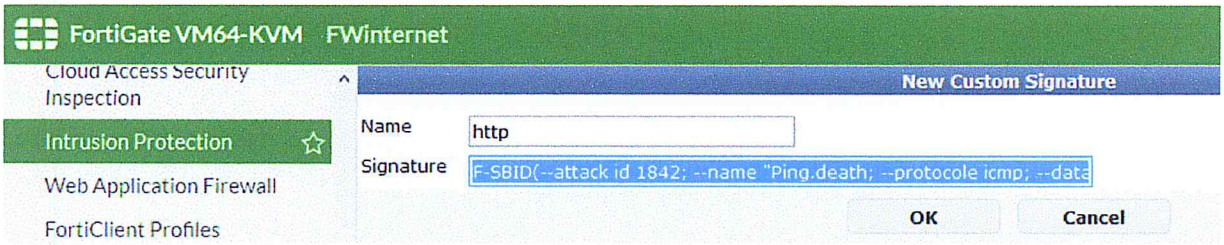


Figure 4.32:Exemple d'ajout d'une signature ips

Remarque :

L'activation d'un profil de sécurité nécessite son application sur la règle de contrôle d'accès correspondante, puis l'activation de l'inspection SSL/TLS/SSH pour prendre en charge l'encapsulation chiffrée, **voir la figure4.33**.

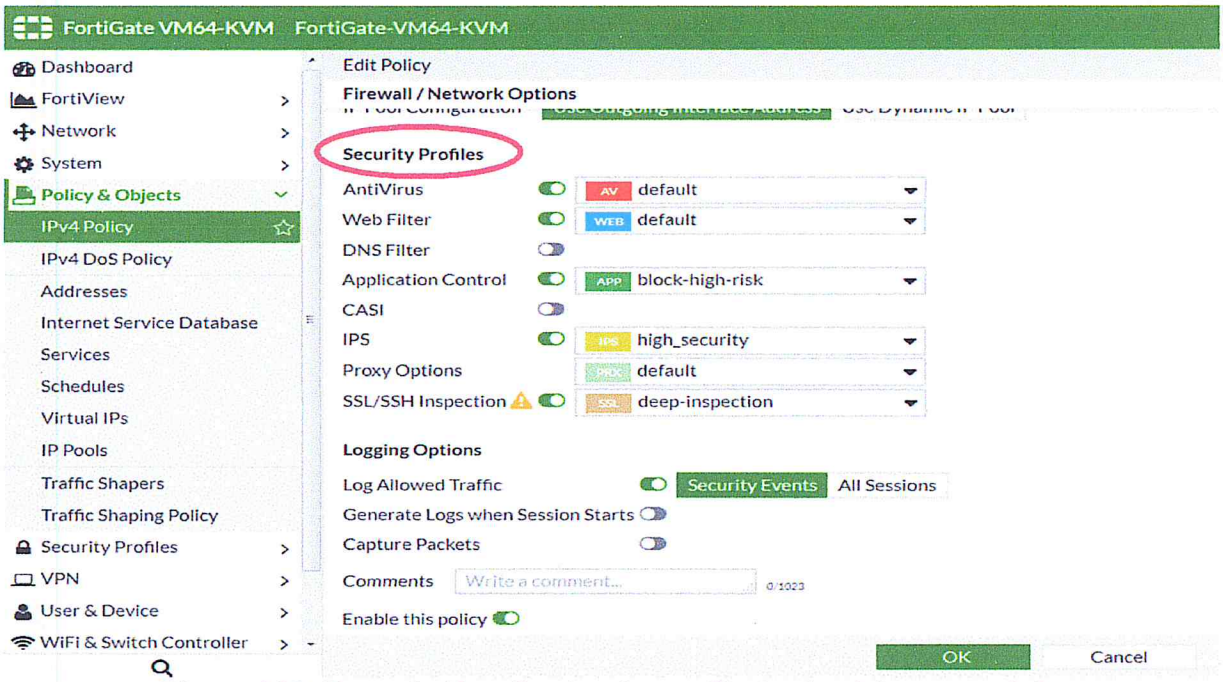


Figure 4.33: Exemple d'application des profils de sécurité sur une règle

g. Protection des attaques DOS :

Cette fonctionnalité permet la protection du réseau des firewalls des attaques par inondations en limitant le nombre de paquet accepté sur une interface donnée.

i. Configuration :

Nous activons la protection DOS sur les interfaces les différentes interfaces du firewall, nous bloquons les inondations de couche 3 et couche 4, le seuil est fixé à 20 paquets.

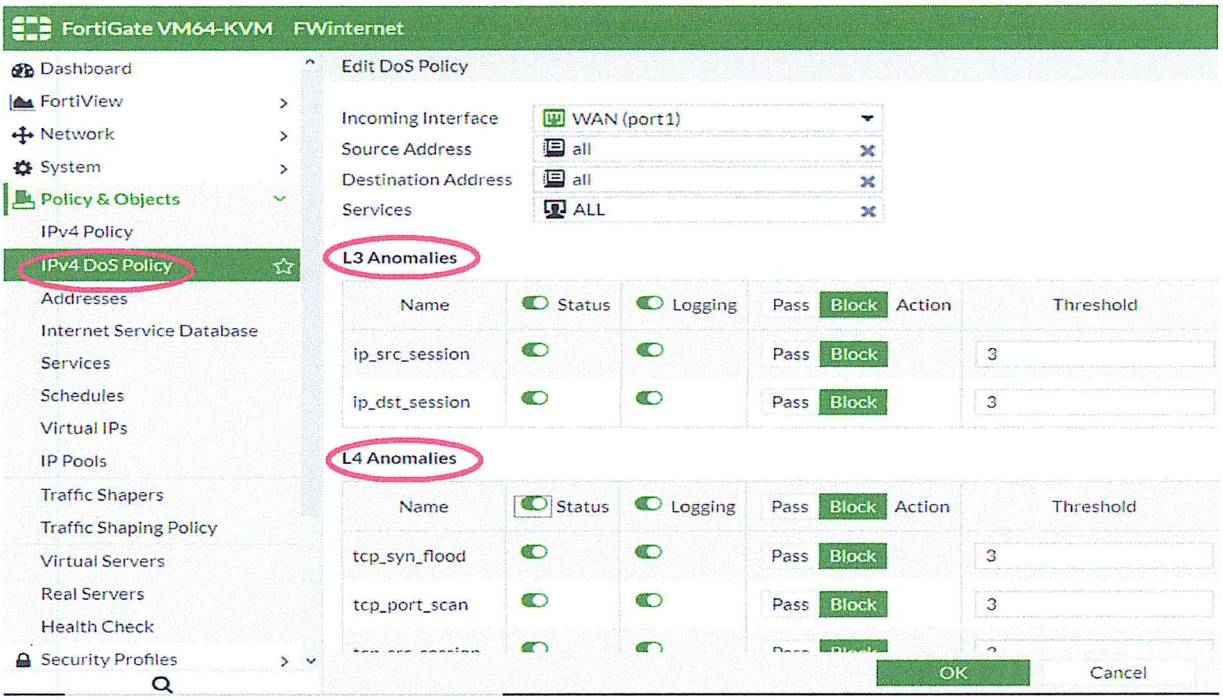


Figure 4.34: Configuration de la protection DOS

ii. Test :

Avant l'activation de la protection DOS sur les interfaces du firewall, nous utilisons l'application LOIC pour effectuer une inondation UDP depuis l'agence, voir **la figure4.35,** vers une machine située au site principal.

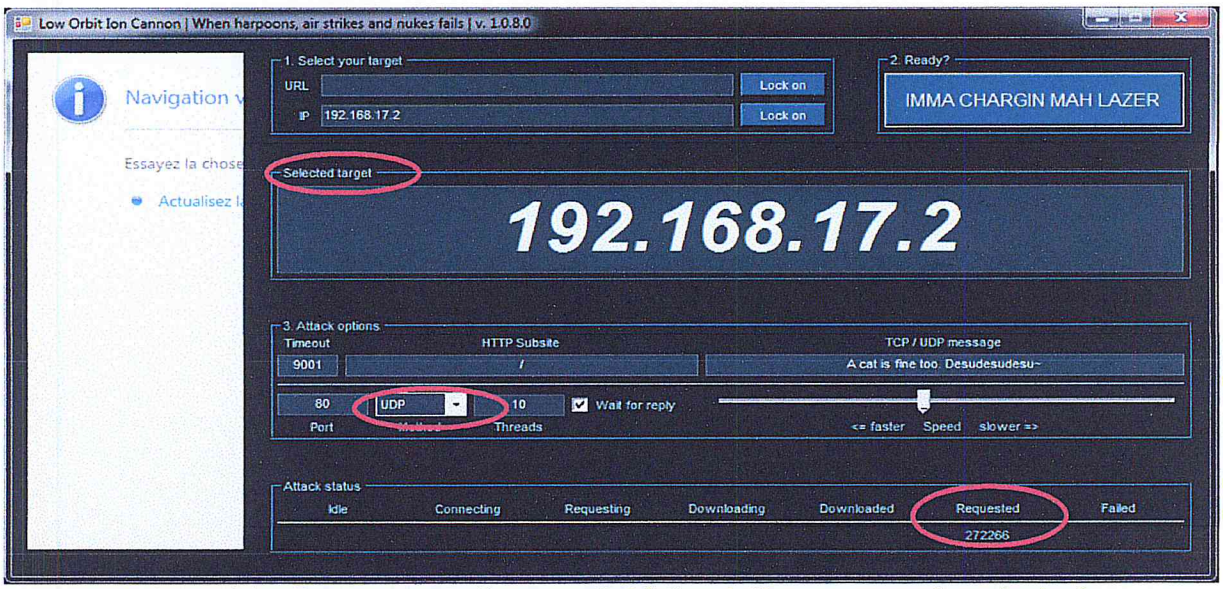


Figure 4.35: Lancement de l'attaque DOS depuis l'agence vers site principal

La figure 4.36 montre que l'hôte devient indisponible.

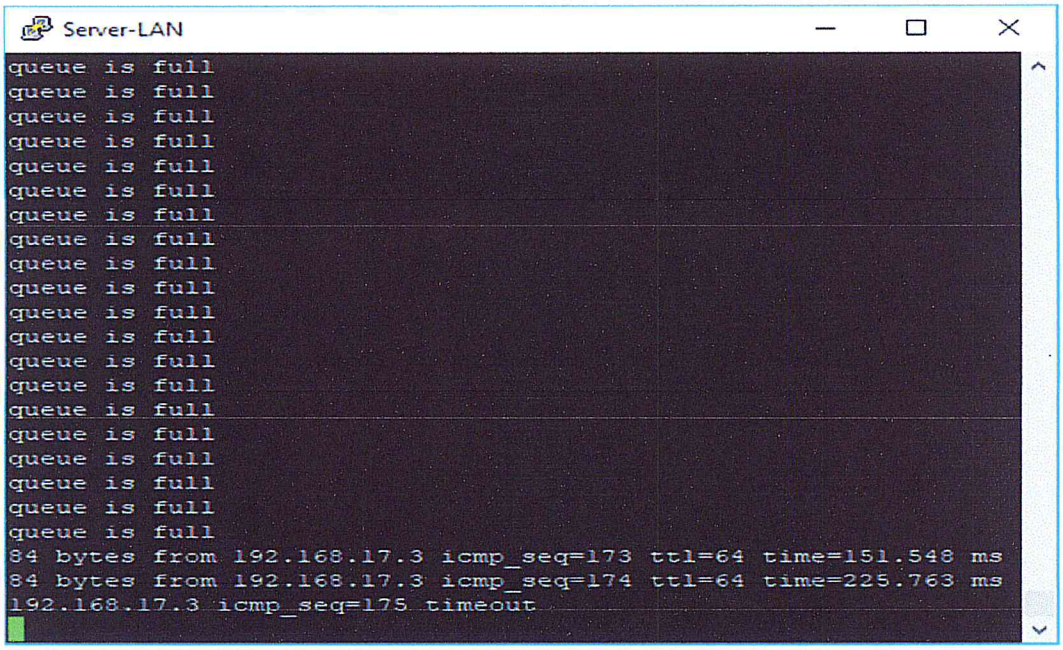


Figure 4.36: Avant l'activation de la protection DOS

Après l'activation de la protection DOS sur les interfaces du firewall, nous reprenons le test précèdent. La figure montre que le serveur est encore actif.

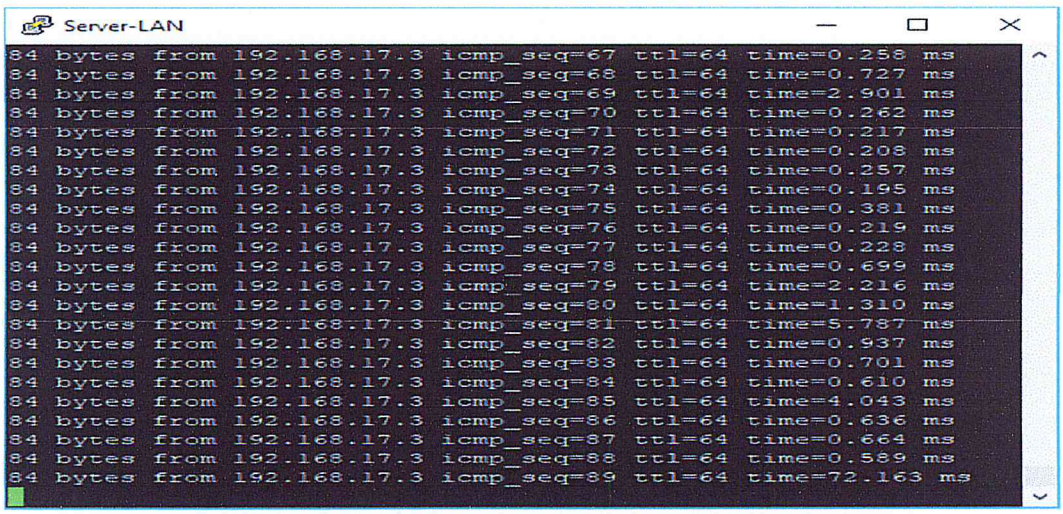


Figure 4.37: Après l'activation de la protection DOS

h. Création d'un réseau VPN SSL :

La création d'un VPN SSL permet l'accès au réseau à distance en toute sécurité.

i. Configuration :

La configuration commence par le choix du mode de connexion à prendre en charge, nous choisissons le mode web. **Voir la figure 4.38**.

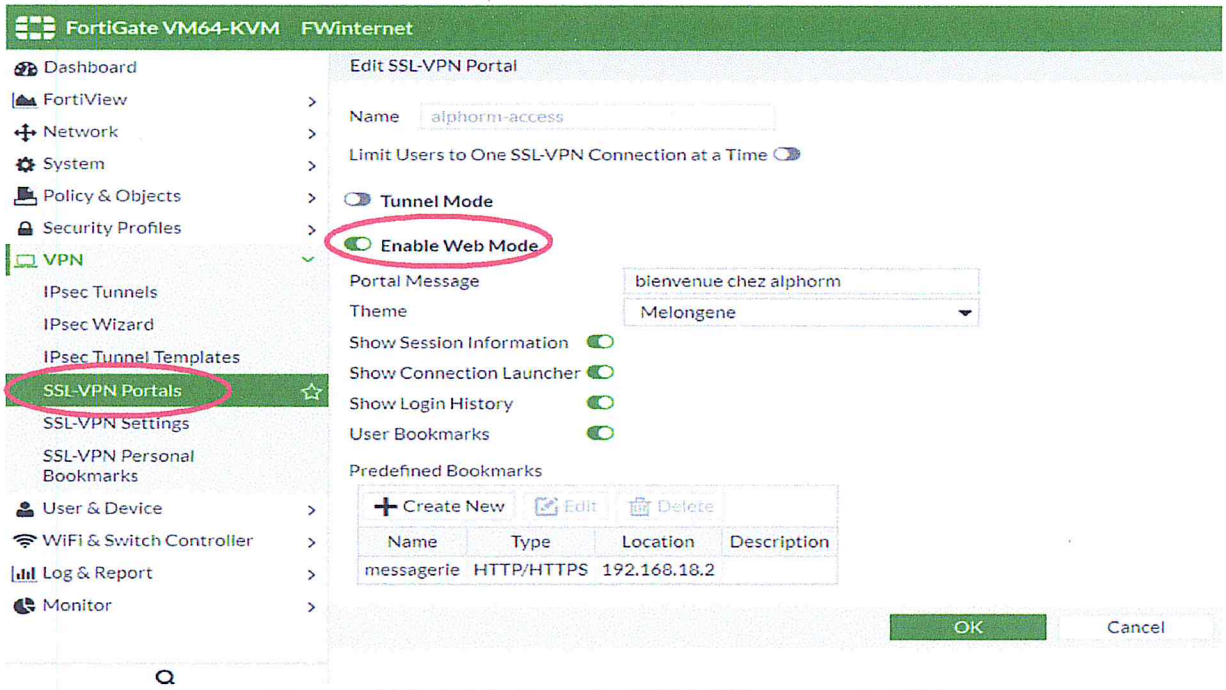


Figure 4.38: Définition du VPN SSL en mode Web

Ensuite, la spécification des paramètres, à savoir l'interface d'écoute sur laquelle le firewall reçoit les paquets et le numéro de port dédié.

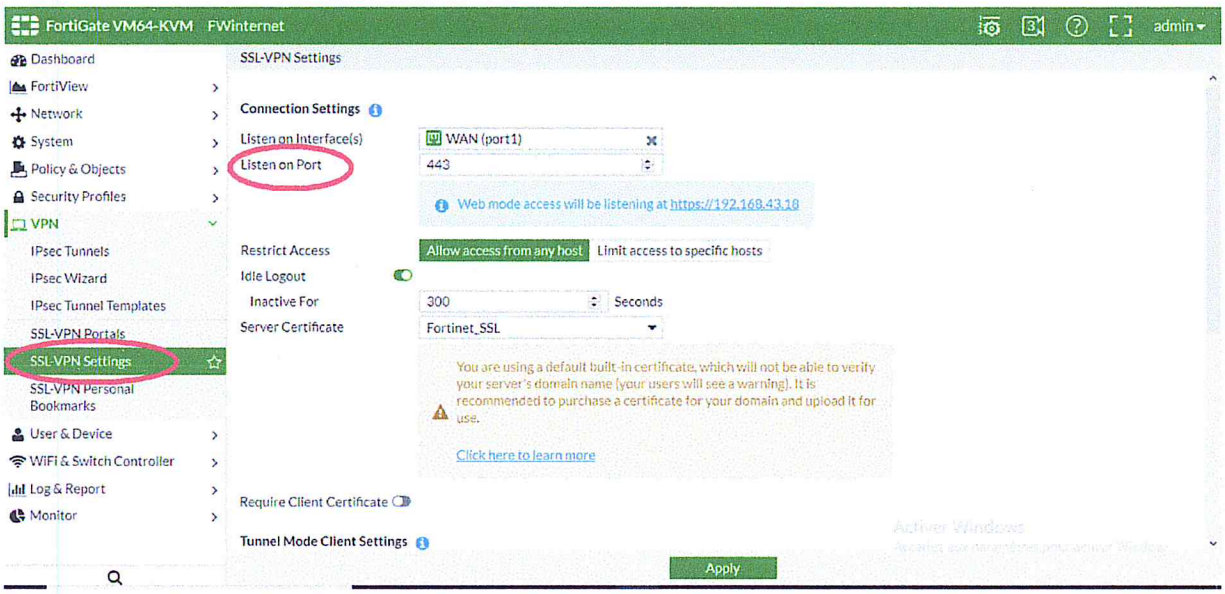


Figure 4.39: Paramétrage du VPN SSL

ii. Test :

Pour se connecter à distance au réseau, il suffit d'accéder au firewall à travers l'adresse configurée précédemment pour le VPN, Voir **la figure 4.40**.

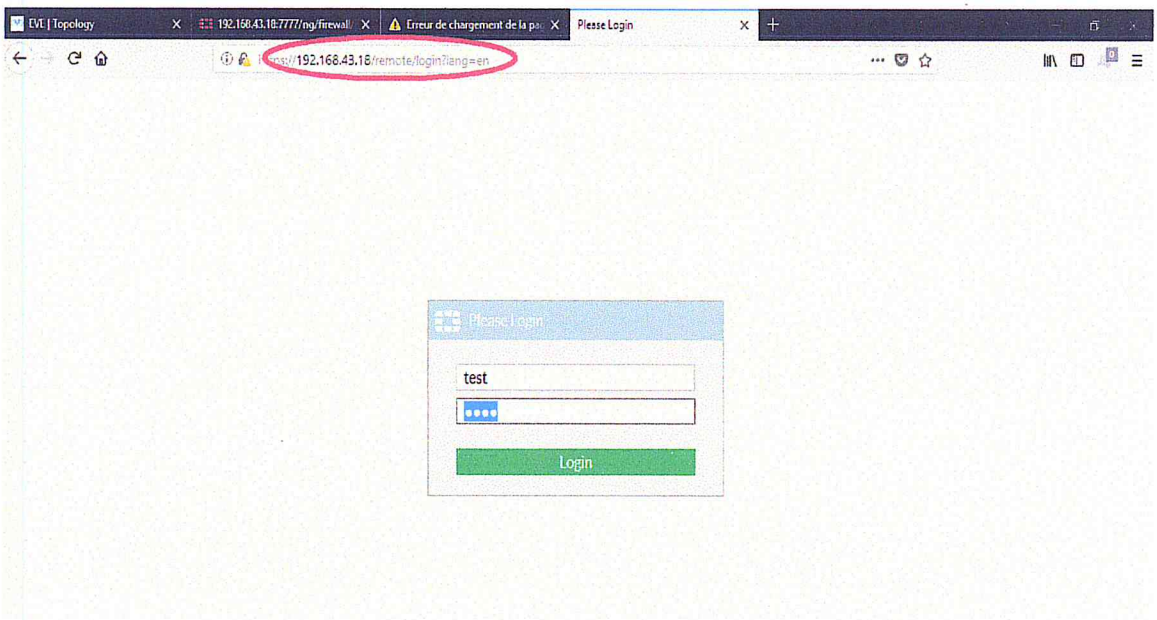


Figure 4.40 : Accès au site principal à distance

Depuis cette page résultante, voir **figure 4.41**, nous pouvons accéder aux ressources réseau comme si nous étions sur site, en utilisons les protocoles proposés par le VPN en mode web.

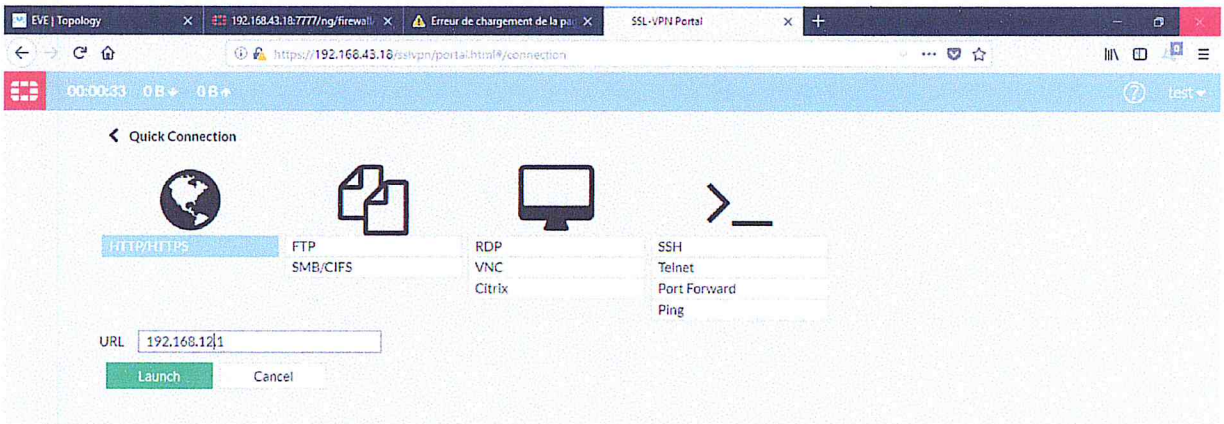


Figure 4.41: Portail VPN SSL

Remarque :

Si le paquet ne correspond à aucune règle de sécurité, il est rejeté par la règle définie par défaut sur le fortigate « Deny implicite ».

5. Conclusion :

Dans ce chapitre, nous avons commencé par simuler une partie du réseau de l'entreprise, ensuite nous avons entamés le déploiement du firewall fortigate pour pouvoir mettre en place les différentes mesures de sécurité. Nous avons commencés par définir de simples règles de contrôle d'accès entre sites et gestion de la bande passante sur les différentes liaisons, puis nous avons implémentés et activés différents profils de sécurité sur les interfaces intranet et extranet, tels que : l'antivirus, le filtrage web, le contrôle applicatif, IPS….ensuite nous avons effectués une protection contre les attaques par déni de services.

Enfin, nous avons paramétrés un VPN d'accès à distance aux ressources réseau. Chacune des fonctionnalités est suivi de test afin de valider les configurations mise en œuvre.

Conclusion générale

La CNEP banque s'est longtemps limité à l'utilisation de plusieurs outils classiques de protection réseau qui répondaient avant, à tous ses besoins ou presque. Mais ceci n'a pas duré longtemps, car l'entreprise doit faire face à de nouveaux enjeux et doit prendre de nouvelle considération. Il s'agit d'une part de l'ouverture de nouveaux services en ligne et d'autre part l'évolution des attaques informatique.

C'est dans cette thématique que s'inscrit notre travail. A savoir « la contribution à la sécurisation du réseau de la CNEP banque ». Il aborde deux volets, le premier volet concerne la proposition d'une architecture sécurisée pour l'extranet. Le second volet consiste au déploiement d'une solution NGFW avec une approche unifiée de gestion des menaces.

Dans un premier temps, nous avons présentés quelques notions théoriques et concepts fondamentaux de la sécurité informatique puis détailler les moyens usuels de protection réseau. Nous avons consacrés un chapitre pour l'étude des principes de bases des firewalls et leur évolution.

Dans un second temps, nous avons menés une étude sur le réseau de l'entreprise qui consiste à décrire son architecture et présenter les mesures de sécurité mise en place, ensuite nous avons portés des critiques sur l'état de la sécurité et la qualité des communications réseau. Ainsi, nous sommes parvenus à proposer une solution permettant de pallier à l'ensemble des vulnérabilités de sécurité réseau de l'entreprise.

Quant à la solution proposée, nous avons commencés par proposer une nouvelle architecture réseau pour l'extranet, en se basant sur l'architecture « DMZ entre deux firewalls » présentée dans l'état de l'art. Nous l'avons améliorés, en partitionnant la DMZ en sous réseaux différents et regrouper ainsi les serveurs dans les DMZs par niveau de sensibilité, nous avons également opérés à une redondance des firewalls, en les faisant fonctionner en mode redondance passive. Ensuite, nous avons optés pour le déploiement d'un NGFW avec une approche unifiée de gestion des menaces.

Enfin, nous avons implémentés notre solution dans un environnement de test. Il s'agit de l'émulateur réseau de nouvelle génération EVE, en utilisant Fortigate comme firewall UTM pour la mise en place des mesures de sécurité. A l'issue de nombreux tests sur les différentes

mesures de sécurité mise en œuvre, nous avons démontrés l'efficacité de l'adoption d'une solution de gestion de menace unifiée.

A cet effet, nous pouvons dire que nous avons atteint 80% de nos objectifs de réalisation. Le projet était une bonne occasion pour enrichir et développer nos connaissances non seulement sur le plan théorique et surtout sur le plan pratique.

Cependant, de nombreuses **perspectives** et améliorations qui s'orientent dans plusieurs directions peuvent être envisagées, nous citons :

- La mise en place d'un VPN IP sec au niveau de l'intranet (VPN site à site), entre les firewalls des différents sites plutôt qu'entre les routeurs afin de protéger les communications en interne
- L'ctivation de la protection WAFs pour renforcer la protection, face aux menaces liées aux applications web.
- Filtrage des spams et gestion des mails commerciaux non sollicités.
- Implémentation de nouveaux algorithmes de protection DOS au niveau des routeurs, tels que : Traceback, Poseidon.

Bibliographie

(1) Chaouachi, A. (2015). « Implémentation d'une solution de sécurité avec une zone démilitarisée ». Editions universitaires européennes. Allemagne.

(2) Dromard, D., Seret, D. (2018). « Sécurité dans les réseaux », encyclopaedia-universalis.23.

(3) Bendahmen, A. (2011). « Installation et configuration d'un firewall ».

(4) BOUCHERBA, K., ZIANE, S. (2015). « Mise en place d'un pare-feu d'entreprise open source PfSense ». Tlemcen.

(5) Ayari, A. (2015). « Audit de Sécurité du Système Informatique de MTIC ». Tunisie.

(6) Abid, Y., Belhocine, M. (2015) « Proposition d'une architecture réseaux sécurisée pour l'université A.Mira de Bejaïa ». Bejaïa.

(7) Ghernaouti, S. (2013). « securité informatique et réseau ». Dunod. paris.

(8) Jean-Francois, P., Jean-Philipe, B. (2013). « Sécurité Informatique ». Dunod, Paris.

(9) Jean-Francois, C. (2012). « La sécurité Informatique Dans la petite entreprise ». Dunod. Paris.

(10) https://www.linkedin.com

(11) https://www.securiteinfo.com

(12) https://securelist.fr

(13) http://www.eve-ng.net

(14) https://cyberstat.kaspersky.com

(15) https://www.putty.org

(16) https://my.vmware.com

(17) https://www.fortinet.com/fr

(18) http://www.encyclopaedia-universalis.fr

(19) https://www.nbs-system.com

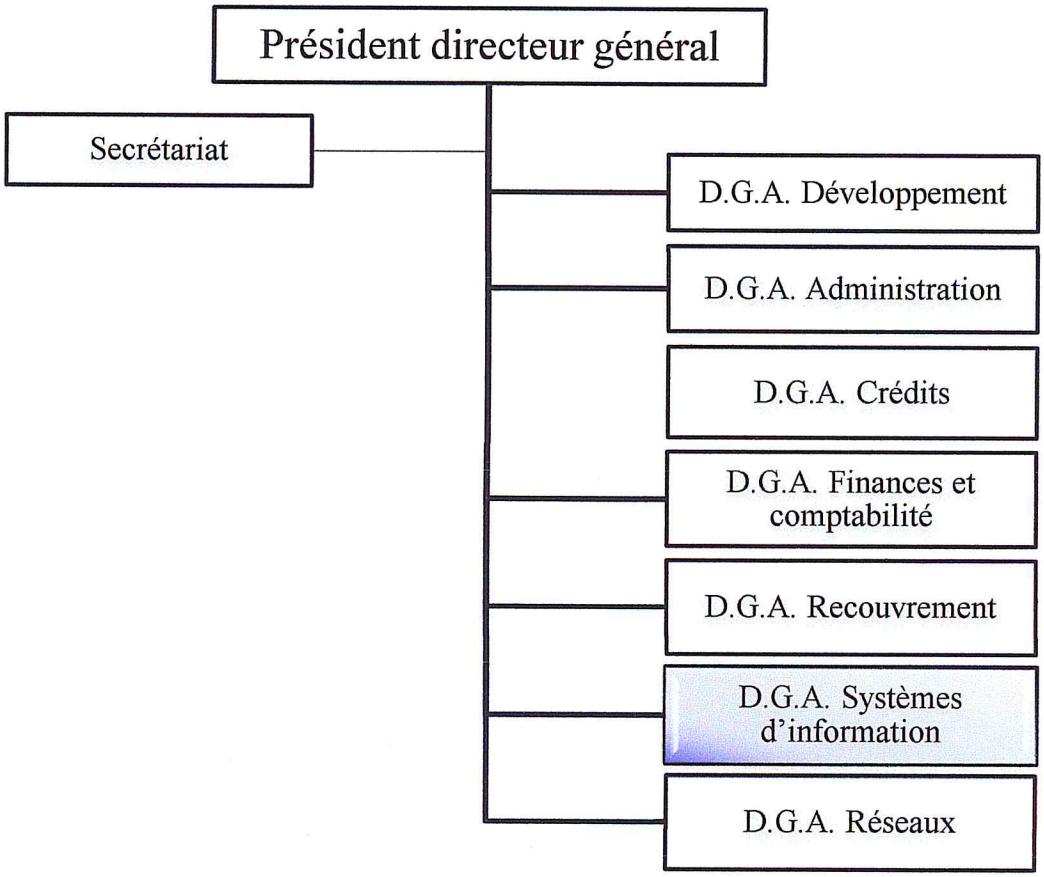
(20) https://www.sophos.com

ANNEXE
Présentation de l'organisme d'accueil

1. Présentation de la Caisse Nationale d'Epargne et de Prévoyance :

La Caisse Nationale d'Epargne et de Prévoyance a été instituée par la loi n°64-227 du 10 août 1964 portant la création et fixant les statuts de la Caisse Nationale d'Epargne et de Prévoyance, parue dans le Journal officiel n°66 du vendredi 14 août 1964 de la République Algérienne Démocratique et Populaire.

La CNEP-Banque est un établissement public spécialisé dans la collecte de l'épargne et les crédits immobiliers aux particuliers destinés aux Algériens résidant en Algérie et à l'étranger. Elle est constituée de 217 agences d'exploitation et 14 directions régionales réparties à travers le territoire national, la CNEP-Banque est présente également au niveau du réseau postal pour l'épargne des ménages.



2. Présentation de la DGA/SI :

La mission principale de la DGA/SI (Direction Générale Adjointe Chargée des Systèmes d'Information) est de doter la banque d'un système cohérant d'information, totalement sécurisé et exploitable par toutes les structures, ce qui lui permet d'assurer un développement permanent et positif pour l'ensemble de ses activités et d'atteindre les objectifs tracés.

Actuellement quatre directions centrales travaillent sous l'autorité de la DGA/SI qui sont :

- La Direction des Etudes et des Applications Informatiques.
- La Direction de l'Exploitation et de l'Assistance aux Utilisateurs.
- La Direction des Instruments de Paiement.
- Département de la Maintenance Réseau, Sécurité et Télécommunication.

3. Présentation du DMRST :

Ce département rattaché à la direction générale adjointe chargée de systèmes d'information (DGA/SI), il est constitué de trois services : service de maintenance, service réseau et télécom et le service sécurité informatique.

➢ Le service de maintenance est chargé de :

- Gestion du parc informatique :
  - Vérification de la mise en marche des équipements informatiques.
  - Installation et configuration des ordinateurs et serveurs (hardwares et softwares).
- Gestion (maintenance et configuration) de la plateforme infrastructure :
  - Serveur *Structured Query Language (SQL).*
  - Serveur Active directory (AD) stratégie de compte, dns, dhcp.
  - Server Exchange (messagerie).
  - SCOM.
  - Serveur Backup (sauvegarde des données).

➢ Le service réseau et télécom est chargé de :

- Installation (hardwares et softwares), configuration et administration des équipements réseaux.
- Maintenance et dépannage de l'infrastructure LAN / WAN.
- Suivi et mise en service du Réseau en étroite collaboration avec Algérie télécom.
- Elaboration des cahiers des charges suivantes les besoins internes de la CNEP banque en termes d'upgrade équipements ou de dépoilement de nouvelles solutions.

➢ Le service sécurité informatique est chargé de :

- ***Antivirus :*** gestion du parc informatique (mise à jour / analyse etc.) via une console centralisé.
- ***Pare-feu :*** gestion des accès des utilisateurs aux ressources protégées ou à internet Filtrage accès page web.
- ***SCOM Monitoring :*** suivi des erreurs & évènement & gestion des logs au niveau des serveurs.

L'organigramme du DMRST est présenté par la figure suivante :

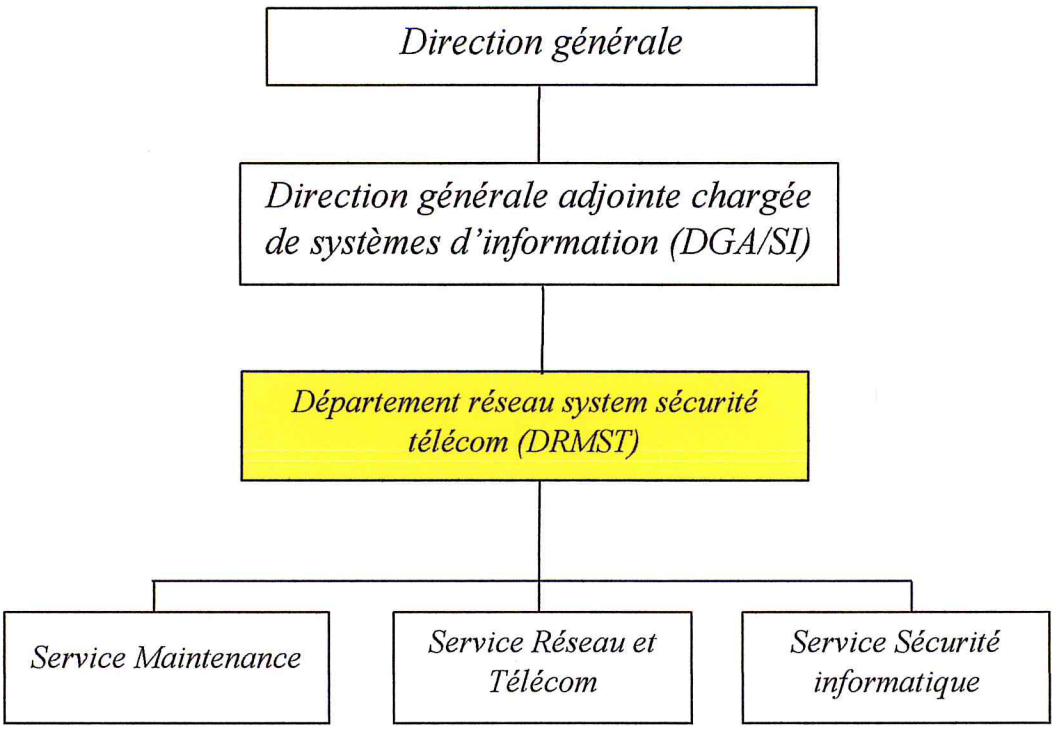


Figure : Organigramme (DRMST)