MEMOIRE DE PROJET DE FIN D'ETUDES

Pour l'obtention du diplôme de master
Systèmes Microélectroniques, de Télécommunications et de l'Informatique Industrielle

L'audit de sécurité du réseau Marsa Maroc

Réalisé par :

- *Asmaa EL GUERAA*
- *Ibtissam DANI*

Encadré par :

- *Mr. Ali SQQALI*
- *Pr. Fatiha MRABTI*
- *Pr. Khalid ZENKOUAR*

Soutenu le : 23 Juin 2011

Devant le jury composé de :

Pr. N.ES-SBAI	***Présidente***
Pr .F. MRABTI	***Encadrant (FST.Fés)***
Pr .K. ZENKOUAR	***Encadrant (FST.Fés)***
Pr. A.MECHAQRANE	***Professeur (FST.Fés)***

ANNEE UNIVERSITAIRE : 20010/2011

Remerciements

Tout d'abord, nous remercions DIEU qui garde toujours un œil bien veillant sur nous.

Nous tenons à exprimer nos sincères remerciements avant tout à nos encadrants techniques.

Mme.Fatiha LAMRABTE et Mr.Khalid ZENKOUAR pour leur disponibilité, leur collaboration, et leurs directives qu'il n'a cessé de prodiguer tout au long de ce projet.

Mr.Ali SQALLI pour sa bienveillance, ses compétences, son aide et son soutien moral, ainsi que pour la confiance dont il a toujours fait preuve à notre égard.

Nous remercions tout le staff d'INTELCOM qui nous a fourni tous les moyens afin de passer notre PFE dans les meilleures conditions, notamment **Mr. Mohamed LOUHAB** et **Mr.LAHCEN** pour leurs aides et leurs sympathies.

Nous profitons de ces quelques lignes pour dire merci à la direction et le département Génie Electrique de FST de Fès, particulièrement Mr. **E.ABARKAN** le chef de filière Master SMTII pour son aide et son soutien ainsi que tout le corps professoral.

Nos vifs remerciements s'adressent également aux membres de jury qui ont accepté d'évaluer notre projet de fin d'études.

Que tous ceux et celles qui ont contribué de près ou de loin à l'accomplissement de ce travail trouvent l'expression de nos remerciements les plus chaleureux.

Sommaire

Index des figures

Index des Tableaux

Acronymes

A

- **AAA :** Authentification, Authorization,Accounting.
- **AD:** active directory

C

- **CDP:** Cisco Discovery Protocol
- **CIP:** Centre Informatique de Port
- **CTA :**cisco trust agent

D

- **DEPC:** Département d'Exploitation au Port de Casablanca
- **DTP :** Département Trafic Polyvalent
- **DTC :** Département Trafic Contener
- **DMZ :** Démilitarisation Zone

E

- **EDI :** Echange de Données Informatisée

F

- **FO :** Fibre Optique
- **FCOE :**fibre chanel over Ethernet
- **FH:**faisceau hertzien

G

- **GPO:** Group Policy Objet

L

- **LS :** liaison spécialisé
- **LAN :** local area network

M

- **MAN: metropolitan area network**

N

- **NAC:** network admission control

P

- **PAI :** le Point d'accès Internet.

Q

- **QOS :** Qualité de service

I

- **IP :** Internet Protocol
- **IPS :** *Intrusion Prevention Systems*

V

- **VLAN :** Virtual Local Area Network

S

- **SNMP**: Simple Network Management Protocol
- **SSG:** Secure Services Gateway

T

- **TOIP:** Telephony over Internet Protocol
- **TLV:** type length value
- **TOR:** top of the rack

U

- **URL:** Uniform Resource Locator

Introduction Générale

Avec le développement de l'utilisation d'Internet, de plus en plus d'entreprises ouvrent leur Système d'Information à leurs partenaires ou leurs fournisseurs. Cette ouverture vers l'extérieur conditionne des gains de productivité et de compétitivité. Il est donc essentiel de connaître les ressources de l'entreprise à protéger et de maîtriser le contrôle d'accès et les droits des utilisateurs du Système d'Information.

Conscient de ce problème, la société Marsa Maroc qui gère le port de Casablanca a lancé un audit afin d'améliorer la sécurité et la disponibilité de son système réseau. Dans ce cadre, la société Intelcom qui a pour mission principal, la mise à niveau et la sécurisation des infrastructures réseaux et systèmes, a pris en charge l'audit de sécurité du réseau de la société Marsa Maroc.

La finalité de notre projet est donc de proposer une architecture réseau optimale en termes de sécurité, disponibilité, d'évolutivité et de qualité de service (QOS), pour la mise à niveau du réseau informatique de Marsa Maroc.

Notre projet s'articule autour de deux axes principaux:

- **La mise en place d'une architecture globale du réseau informatique permettant de supporter les besoins actuels et futurs (disponibilité, évolutivité et Qualité de Service)**

- **L'interconnexion d'une manière sécurisée du DEPC (Département d'Exploitation de Port de Casablanca) aux différents départements (siège, partenaire, Internet…).**

Le présent mémoire comporte quatre chapitres:

- **Le premier chapitre sera consacré à la présentation de l'organisme d'accueil (Intelcom) et le contexte général du projet.**

- **Le second chapitre présentera les concepts théoriques qui regroupent les technologies et les infrastructures qui seront déployés pour la réalisation du projet.**

- **Au cours du troisième chapitre, nous allons présenter l'étude de l'existant concernant le réseau local (LAN) et métropolitain (MAN) de Marsa Maroc, ainsi que l'identification des anomalies et des menaces potentielles.**

- **Dans le dernier chapitre, nous proposerons les recommandations qui permettrons d'obtenir une architecture réseau optimale en termes de qualité de service, sécurité et disponibilité.**

Contexte général du projet

L'objectif de ce premier chapitre est de présenter le cadre général du projet dans lequel on donne une brève présentation de l'organisme d'accueil de la société INTELCOM, ensuite on présente la démarche et la méthodologie du projet.

I. Présentation de l'organisme d'accueil

1. Introduction

Intelcom est une société anonyme marocaine, fondée en 1988, et qui a ouvert en juillet 2001 la majorité de son capital au groupe SATEC (Sistemas Avanzados de Tecnologia, S.A), leader en Espagne et au Portugal dans les Réseaux et Télécoms.

Intelcom est précurseur dans le domaine des nouvelles technologies de l'information. Elle a mis en œuvre les premiers réseaux pré-câblés, les premiers réseaux locaux à fibre optique, les premiers réseaux basés sur IP et les plus grands réseaux bancaires au Maroc. Intelcom a également réalisé le réseau Internet National, le premier provider Internet Atlasnet et le premier opérateur de commerce électronique Maroc Télécommerce.

2. Fiche signalétique

Dénomination: Intelcom (Ingénierie des Télécommunications)
Capital social: 20 M Dhs
Siège social: Rabat
Agence: Casablanca
Effectif: 135
Chiffre d'affaires 2006: 126 M DHs

3. Organigramme d'INTELCOM:

L'Organigramme fonctionnel d'INTELCOM est présente ci–dessous:

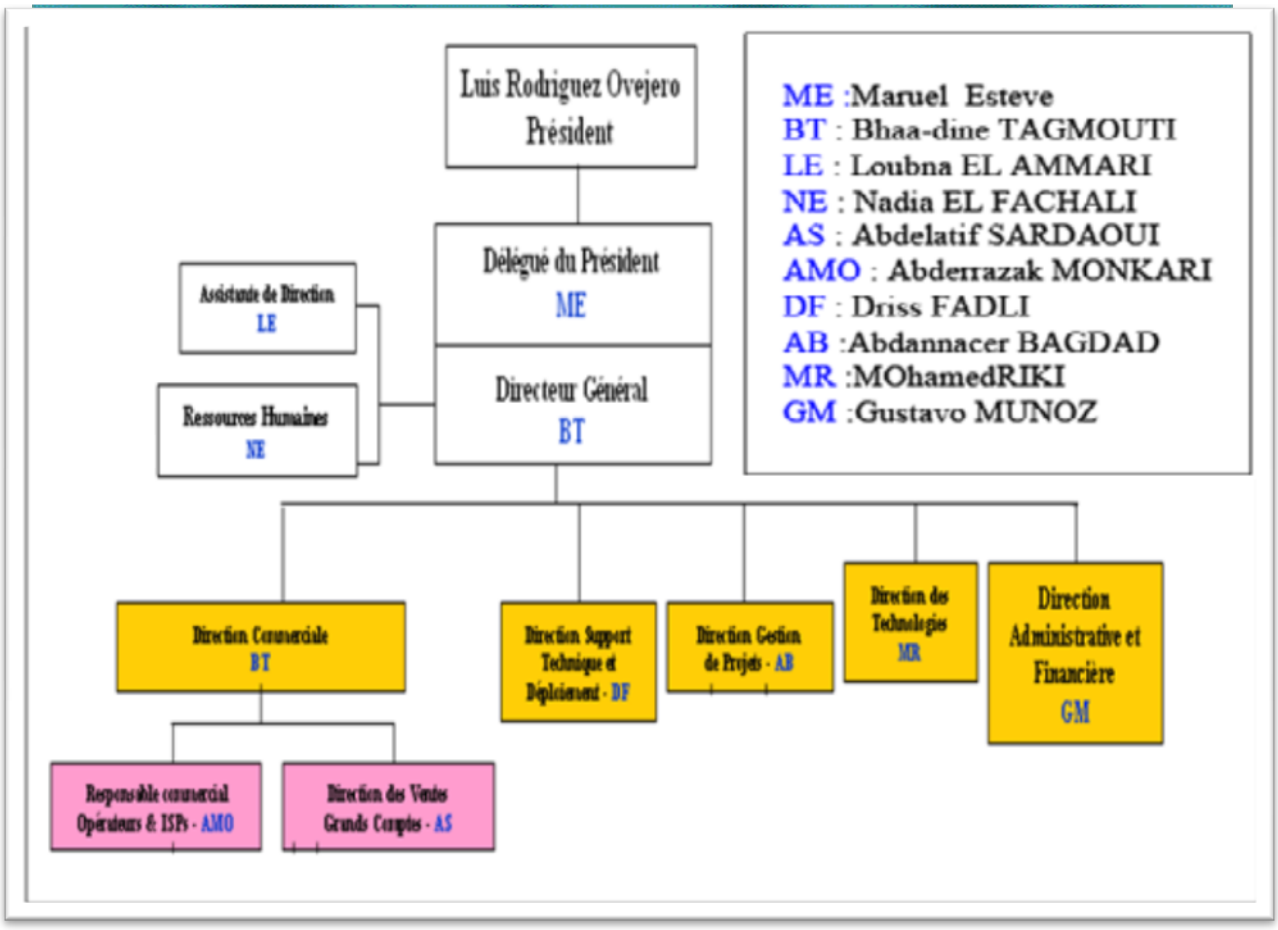


Figure 1 : L'Organigramme fonctionnel d'INTELCOM

4. Services offerts

Acteur depuis de nombreuses années auprès des plus grands comptes au Maroc, Intelcom offre son expérience et son expertise afin de permettre à ses clients de choisir et d'élaborer les solutions les mieux adaptées à leurs métiers, d'optimiser la mise en œuvre de leurs projets et d'obtenir rapidement un retour sur investissement.

Ainsi, dans le cadre de ses prestations de service, Intelcom offre un ensemble de services à forte valeur ajoutée. Nous citons en particulier:

- **L'infrastructure réseaux et télécoms,**
- **La sécurité,**
- **Applications Internet/intranet,**
- **Administration des réseaux.**

II. Objectif du stage

Le projet «Audit de sécurité du réseau» a pour but de voir l'état des lieux du réseau en termes de sécurité, disponibilité, évolutivité et présenter les recommandations possibles

de manière à avoir une architecture réseau complètement optimale qui réponds aux besoins en termes de qualité et de coût.

En vue de réaliser les objectifs susmentionnés, une méthodologie de conduite de projet a été adoptée.

III. méthodologie du stage

Afin de réaliser les différents objectifs fixés du projet, deux étapes principales ont été identifiées:

- **Etape 1: Etude de l'existant**

Cette étape est primordiale, elle consiste à établir « un état de lieu » du réseau informatique permettant de connaître son état initial ainsi que son aspect physique et logique.

Durant cette étude, une cartographie « schéma » détaillée de la topologie physique a été réalisée pour avoir une vue d'ensemble du réseau permettant de le cerner en sa totalité, ainsi que les outils de protections déjà mis en place.

Nous nous sommes basés dans le diagnostique du réseau sur les critères suivants :

- ✓ **Evaluer le degré de sécurité des données,**
- ✓ **Détecter les performances et faiblesses du réseau informatique,**
- ✓ **Avoir une vision claire sur les solutions qu'il faut mettre en place pour plus d'efficacité.**

- **Etape 2: analyse, spécifications et planification**

Cette étape permet de définir le compte tenu des résultats du diagnostic, et l'ensemble des objectifs qu'il faut atteindre dans le cadre du projet de mise à niveau et de sécurisation du réseau.

En fonction des objectifs qui ont été mis en évidence, il a fallu analyser, concevoir et déterminer la meilleure solution globale. Le choix de cette solution a été effectué à l'issue de plusieurs réunions avec les responsables de projet à Marsa Maroc et Intelcom.

Le choix de la solution globale s'est basé sur les éléments suivants:

- ✓ **Adaptation par rapport aux besoins,**
- ✓ **Transparence pour les utilisateurs de l'architecture actuelle du réseau,**
- ✓ **Evolutivité,**
- ✓ **Coût.**

Conclusion

Dans ce chapitre nous avons décrit le contexte général du projet dont on a présenté en bref la société d'accueil, la problématique et les démarches qu'on va suivre pour la mise en place des nouvelles solutions technologiques.

Dans le chapitre suivant, on va aborder les concepts théoriques de la sécurité du réseau informatique.

Chapitre 2

Le concept théorique

Ce chapitre présente les différents concepts théoriques à savoir :

- **La conception des réseaux locaux(LAN),**
- **La politique de sécurité,**
- **L'administration du parc informatique.**

I. Réseaux locaux: architecture et sécurité

1. Définition et architecture d'un LAN

Un réseau local (LAN: Local Area Network) est un groupe d'ordinateurs connectés entre eux et situés dans un certain domaine géographique. Les réseaux locaux peuvent être de taille très variée; vous pouvez avoir un réseau avec deux ordinateurs côte à côte dans la même pièce, ou bien un réseau avec plusieurs centaines d'ordinateurs dans un même bâtiment.

Les réseaux locaux sont des infrastructures complexes et pas seulement des câbles entres stations de travail.

- La liste des composants d'un réseau local est :

✓ Le câblage,

✓ Le système d'exploitation ou bien gestionnaire de réseaux,

✓ Le ou les serveurs de fichiers,

✓ Le système de sauvegarde,

✓ Les ponts, les routeurs ou passerelles le système de gestion et d'administration du réseau,

✓ La méthode d'accès,

✓ Les protocoles du réseau.

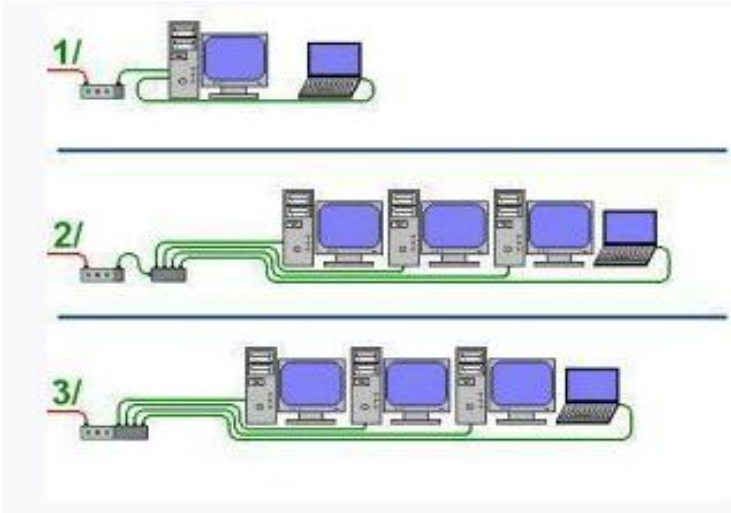


Figure 2: Exemple d'un schéma LAN

2. Politique et mécanismes de sécurité

Tout équipement connecté à un réseau informatique est potentiellement vulnérable à une attaque, ce qui nous mène à réfléchir à une politique de sécurité.

2.1 Les infections informatiques

Une infection ou un virus est un petit programme informatique situé dans le corps d'un autre, qui, lorsqu'on l'exécute, se charge en mémoire et exécute les instructions que son auteur a programmé. La définition d'un virus pourrait être la suivante:

«Tout programme d'ordinateur capable d'infecter un autre programme d'ordinateur en le modifiant de façon à ce qu'il puisse à son tour se reproduire ».

Le champ d'application des virus va de la simple balle de ping-pong qui traverse l'écran au virus destructeur de données, ce dernier étant la forme de virus la plus dangereuse. Ainsi, étant donné qu'il existe une vaste gamme de virus ayant des actions aussi diverses que variées, les virus ne sont pas classés selon leurs dégâts mais selon leur mode de propagation et d'infection.

On distingue ainsi différents types de virus :

- **Les vers sont des virus capables de se propager à travers un réseau**
- **Les chevaux de Troie (troyens) sont des virus permettant de créer une faille dans un système (généralement pour permettre à son concepteur de s'introduire dans le système infecté afin d'en prendre le contrôle)**
- **Les bombes logiques sont des virus capables de se déclencher suite à un événement particulier (date système, activation distante, ...).**

2.2 Politique de sécurité

2.2.1 Définir une politique de sécurité

La politique de sécurité peut être définie comme étant un ensemble d'orientations suivies par une organisation en termes de sécurité, à ce titre elle doit être élaborée au niveau de la direction de l'organisation concernée; car elle concerne tous les utilisateurs du système.

La définition d'une politique de sécurité réseau fait intégralement partie de la démarche sécuritaire de l'entreprise. Elle s'étend à de nombreux domaines :

- audit des éléments physiques, techniques et logiques constituant le système d'information de l'entreprise.
- sensibilisation des responsables de l'entreprise et du personnel aux incidents de sécurité et aux risques associés.
- formation du personnel utilisant les moyens informatiques du système d'information.
- structuration et protection des locaux abritant les systèmes informatiques et les équipements de télécommunications, incluant le réseau et les matériels.
- ingénierie et maîtrise d'œuvre des projets incluant les contraintes de sécurité dès la phase de conception ;

- gestion du système d'information de l'entreprise lui permettant de suivre et d'appliquer les recommandations des procédures opérationnelles en matière de sécurité;

- définition du cadre juridique et réglementaire de l'entreprise face à la politique de sécurité et aux actes de malveillance, 80 pour 100 des actes malveillants provenant de l'intérieur de l'entreprise ;

Classification des informations de l'entreprise selon différents niveaux de confidentialité et de criticité.

2.2.2 Principes génériques d'une politique de sécurité réseau

Afin d'éviter un certain nombre d'écueils classiques, une politique de sécurité réseau doit respecter un ensemble de principes génériques. Ces principes permettent notamment à chacun de bien cerner les enjeux de la rédaction d'un document de politique de sécurité, qui n'est pas un document comme les autres.

Un document de politique de sécurité peut être écrit de plusieurs manières, allant d'un texte unique à une infrastructure de politique de sécurité. Le choix d'écrire un ou plusieurs documents est le plus souvent dicté par la taille de l'entreprise. Plus l'entreprise est importante, plus il est intéressant de créer des documents séparés, chaque niveau faisant référence au niveau supérieur.

Petites, moyennes et grandes entreprises s'exposent dans l'absolu aux mêmes risques si elles n'émettent pas de politique de sécurité. La politique de sécurité dicte la stratégie de sécurité de l'entreprise de manière claire et précise. Le fond et la forme sont donc primordiaux.

Quelle que soit la nature de biens produits par l'entreprise, sa politique de sécurité réseau doit satisfaire les points suivants:

- **identification: information permettant d'indiquer qui vous prétendez être. Une identification élémentaire est le nom d'utilisateur que l'on saisit dans un système informatique. Une identification plus évoluée peut être le relevé d'empreinte digitale, l'analyse faciale, rétinienne bref les méthodes biométriques ;**

- **authentification: information permettant de valider l'identité pour vérifier que vous êtes celui que vous prétendez être. Une authentification élémentaire est le mot de passe que vous entrez. Une authentification forte combine une chose que vous possédez, une chose que vous connaissez (code personnel par exemple) et une chose que vous savez faire (par exemple une signature);**

- **autorisation: information permettant de déterminer quelles seront les ressources de l'entreprise auxquelles l'utilisateur identifié et autorisé aura accès ainsi que les actions autorisées sur ces ressources. Cela couvre toutes les ressources de l'entreprise,**

- **confidentialité: ensemble des mécanismes permettant qu'une communication de donnée reste privée entre un émetteur et un destinataire. La cryptographie ou le chiffrement des données est la seule solution fiable pour assurer la confidentialité des données;**

- **intégrité: ensemble des mécanismes garantissant qu'une information n'a pas été indûment modifiée ;**

- **disponibilité: ensemble des mécanismes garantissant que les ressources de l'entreprise sont accessibles pour qui a droit, que ces dernières concernant l'architecture réseau, la bande passante, le plan de sauvegarde …;**

- **non répudiation: mécanisme permettant de garantir qu'un message ne peut être renié par son émetteur;**

- **traçabilité: ensemble des mécanismes permettant de retrouver les opérations réalisées sur les ressources de l'entreprise. Cela suppose que tout événement applicatif soit archivé pour investigation ultérieure.**

2.3 Les solutions et mécanisme de sécurité

2.3.1 Les firewalls

a. Introduction

De nos jours, toutes les entreprises possédant un réseau local possèdent aussi un accès à Internet, afin d'accéder à la manne d'information disponible sur le réseau des réseaux, et de pouvoir communiquer avec l'extérieur. Cette ouverture vers l'extérieur est indispensable... et dangereuse en même temps. Ouvrir l'entreprise vers le monde signifie aussi laisser place ouverte aux étrangers pour essayer de pénétrer le réseau local de l'entreprise, et y accomplir des actions douteuses, parfois gratuites, de destruction, vol d'informations confidentielles,…

Pour parer à ces attaques, une architecture sécurisée est nécessaire. Pour cela, le cœur d'une telle architecture est basé sur un firewall (Pare-feu).

b. Définition

Un pare-feu (Firewall) est un logiciel ou un matériel qui se charge d'établir une barrière entre le monde intérieur et le monde extérieur pour faire barrage aux pirates comme le montre l'exemple suivant:

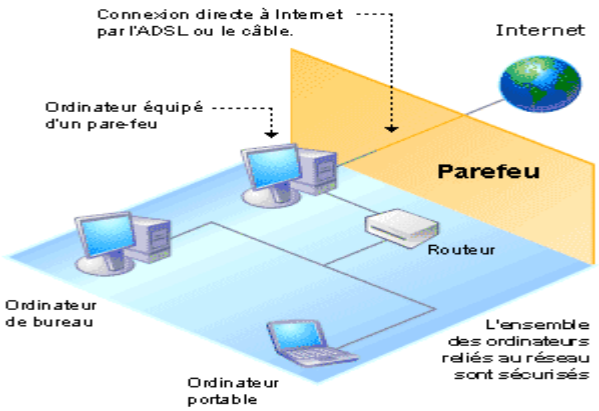


Figure 3: La façon dont le firewall protège le réseau

Rappelons qu'un ordinateur utilise des ports pour communiquer : par exemple, le port 80 est utilisé pour afficher des pages web. Il y a plus de 65000 ports (65536 exactement), soit autant de portes d'entrée dans votre ordinateur qu'un firewall se doit de protéger.

Un pare-feu peut vous permettre de "fermer" les ports et de cette manière, vous rendre invulnérable (ou presque). Il peut aussi restreindre le trafic sortant et applique des restrictions au trafic entrant.

c. Les types de **Firewall**

- **Le pare-feu logiciel et personnel :** il est simple d'utilisation. C'est un logiciel qui contrôle les données entrantes et sortantes. Sachez que Windows XP dispose d'un pare-feu. Nous verrons plus bas comment l'activer. Un firewall logiciel coûte relativement peu cher.
- **Le routeur :** il masque votre adresse IP et vos ports. C'est un périphérique matériel accompagné d'un logiciel qu'il faut mettre souvent à jour. Il est déjà plus cher que le pare-feu personnel. Ce n'est pas un vrai pare-feu dans ce sens que ce n'est pas sa fonction première.
- **Le pare-feu matériel :** Les firewalls hardware les plus simples sont sous forme de boîtier incluant deux connecteurs réseau. Le premier pour relier le réseau interne, le second pour relier l'extérieur.

d. Le blocage de port:

Une IP ne suffit pas pour exécuter des tâches sur un réseau. Il faut des ports, qui vont permettre à l'ordinateur de pouvoir distinguer les différentes sources de données et ainsi exécuter l'application souhaitée.

Plusieurs cas peuvent se présenter, nous vous présenterons les plus fréquents.

- ✓ **D'un client vers le serveur d'une entreprise:**

Nous avons plusieurs clients qui veulent se connecter au serveur web d'une entreprise. Etant donné que c'est un serveur web, seul le port 80 sera accessible et autorisé lorsque les clients voudront se connecter sur le serveur. Le firewall laissera donc passer tout les clients qui veulent voir le site web de l'entreprise. Par contre, les clients qui veulent accéder à une autre porte que la porte 80, par exemple la porte 5631, du serveur ne pourront pas y accéder car le trafic sur ce port n'est pas autorisé. Le firewall leur bloque donc l'accès.

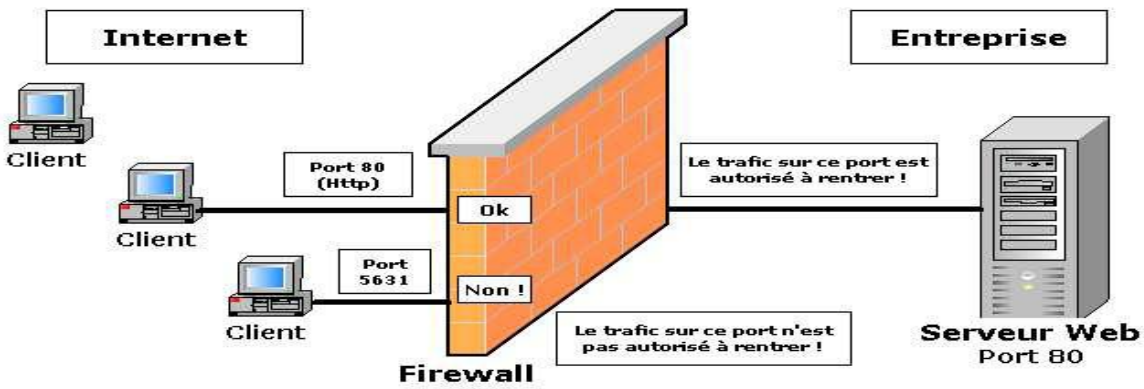


Figure 4 : Le firewall avec un serveur Web

✓ **D'une entreprise vers l'extérieur :**

Nous voici dans l'autre sens. Ici, ce sont les clients de l'entreprise qui veulent accéder à différente application. Dans l'exemple ci-dessous, nous remarquons que les clients peuvent voir des pages web, mais qu'ils ne peuvent pas aller sur Msn Messenger.

En effet, le firewall bloque tout accès au port 1863 aux personnes de l'entreprise. Le port 1863 étant celui utilisé par le programme Msn Messenger.

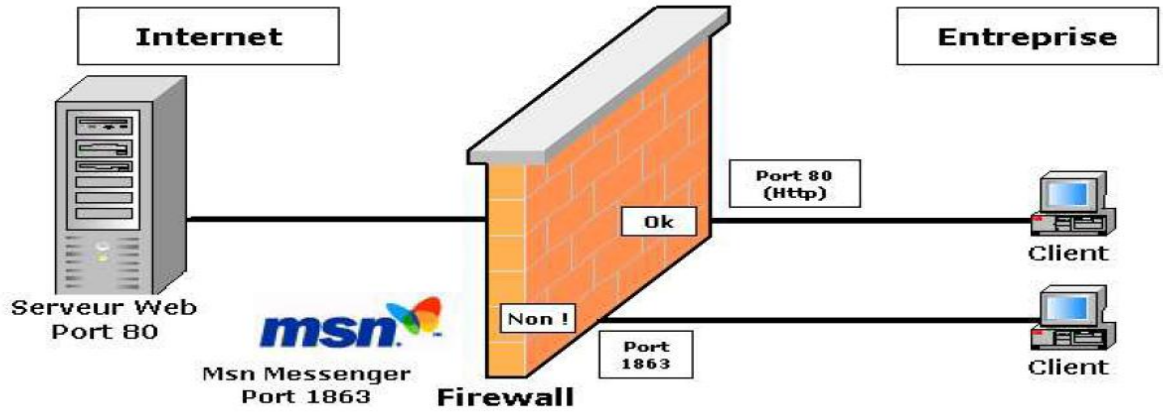


Figure 5 : Protection de Firewall entre l'entreprise et l'extérieur

2.3.2 Filtrage d'URL et de contenu

a. Introduction

Internet apporte la rapidité et la commodité aux activités commerciales quotidiennes, mais il est aussi la source de nombreuses distractions.

Les employés pourraient à tout moment être tentés d'utiliser les connexions de l'entreprise pour faire des achats, chatter, jouer, investir ou consulter un contenu inacceptable. Même des politiques précisant l'utilisation acceptable d'internet sont mises en place, il est primordial de trouver un moyen d'en garantir l'application.

b. Filtrage d'URL

Le filtrage d'URL consiste à analyser certaines informations sur chaque document ou ressource accédée par un utilisateur, ce travail est basé sur l'étude des URL et des keywords. Les logiciels de filtrage travaillent de manière transparente sur le réseau, c'est-à-dire que les scans offrent, en plus d'une grande efficacité, des temps de réponse inégalables. Ils facilitent la surveillance, la gestion et la consignation des données sur le trafic entre les réseaux internes et Internet.

Cette formule stratégique permet d'accroître la productivité et de réduire au maximum les risques en matière juridique et de gestion du personnel.

c. Filtrage de contenu

Le filtrage de contenu regroupe toute une série de technologies avancées qui, à la différence du filtrage d'URL, s'attachent à pénétrer à l'intérieur des documents (le filtrage d'URL se limitant à l'inspection des URL et des mots clés). Les logiciels de filtrage traitent l'information ' à la volée', tout site accédé par un utilisateur est donc nécessairement analysé.

Globalement les systèmes de filtrage appartiennent à deux catégories. Ceux qui analysent le contenu au moment même de l'accès et ceux qui se réfèrent à une classification pré-établie.

Les mécanismes de sécurité présentés jusqu'au là sont la plupart destinés à la sécurisation des réseaux locaux. Mais la plupart des grands organismes ont des réseaux géographiquement éloignés et leur interconnexion ne pourra qu'augmenter la productivité de l'organisme.

2.3.3 Demilitarized zone (DMZ)

On appelle DMZ (Demitarized Zone) un sous-réseau du réseau global à sécuriser comportant en général les serveurs http, ftp, smtp, …, crées dont le but est d'éviter toute connexion directe avec le réseau interne et de prévenir celui-ci de toute attaque extérieure depuis le Web.

Sur un pare-feu, on appelle DMZ une zone qui n'est ni publique, ni interne. Ces zones ne peuvent exister que si le pare-feu possède plus de deux interfaces réseau, une pour la connexion au réseau externe et l'autre pour la connexion au réseau interne. Comme le montre la figure suivante:

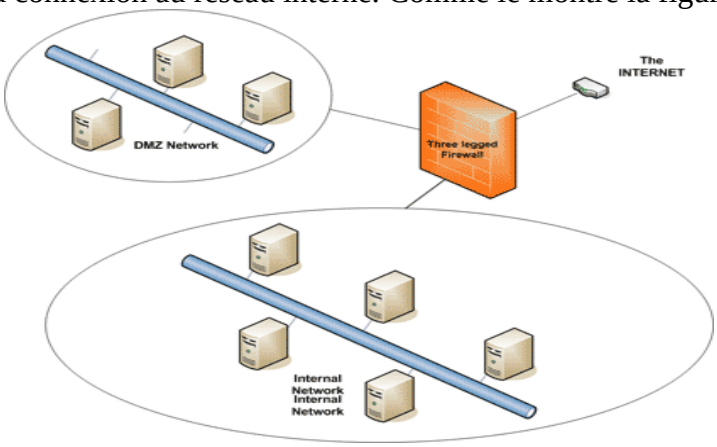


Figure 6 : schéma représente le réseau de DMZ

La mise en place d'une DMZ (avec un Firewall) présente les avantages suivants:

- Possibilité de faire de la **Traduction d'adresse** ou (**NAT-Network Address Translation**), i.e. les adresses privées ne sont pas visibles de l'extérieur car le routeur remplace les adresses sources internes par l'adresse de son interface externe, ce qui permet de garder les adresses internes secrètes et également de dupliquer virtuellement les adresses IP.
- Filtrage des adresses IP pour bloquer un trafic entrant/sortant.
- Isolation de la DMZ: isolement physique des réseaux interconnectés. Un flux direct Internet/Intranet est interdit.
- Définition des règles de filtrage spécifiques à la DMZ et modifiables à tout moment sur le script de configuration.

Par contre, les inconvénients les plus importants sont les suivants :

- La mise en place nécessite une infrastructure lourde en général, surtout si on met en place des redondances pour augmenter la sécurité.
- Coût généralement élevé.

2.3.4 Outils d'évaluation des performances du réseau

La plupart des outils nous aident à mesurer la charge du réseau et à déterminer l'utilisation du réseau. Certains de ces outils, comme les outils de contrôle du trafic logiciel et les analyseurs de

protocole, sont gratuits. D'autres, tels les outils de diagnostic de poche, sont plus conviviaux et portables. Quel que soit l'outil utilisé, il vous fournit des informations utiles sur le statut du réseau.

Plusieurs outils logiciels relativement économiques sont désormais disponibles et offrent des fonctionnalités de suivi et des analyseurs de trame.

- **Outils de contrôle du trafic et analyseurs de trame**

→**Outils de contrôle**: Les outils de contrôle nous permettent de mesurer l'utilisation du réseau, la distribution de protocole et l'utilisation de la bande passante.

→**Analyseurs de trame:** On utilise les analyseurs de trame pour étudier le contenu des trames du réseau afin de procéder à un dépannage réseau complexe. Les analyseurs de trame peuvent également simuler du trafic sur le réseau afin de nous aider à planifier une croissance future. Le Moniteur réseau constitue un exemple classique de ce type d'outil.

→**Analyseurs de trame assistés par matériel:** Les analyseurs de trame assistés par matériel sont généralement des outils demandant des connaissances accrues et utilisés pour résoudre et analyser les réseaux. Ils sont généralement exécutés sur un ordinateur personnel et comportent une carte réseau spécifique. Sniffer, de Network Associates, est le produit le plus connu parmi cette gamme d'outils.

→**Logiciel d'administration réseau**: La plupart des plates-formes d'administration réseau SNMP (Simple Network Management Protocol) sont disponibles de nos jours et la plupart des matériels réseaux récents permettent de collecter des statistiques réseaux. Vous utiliserez généralement la fonction de contrôle à distance (RMON) SNMP pour rassembler des informations sur les ports de commutation individuels. Voici quelques exemples de plates-formes d'administration réseau : CiscoWorks de Cisco Systems, Optivity de Nortel Networks et OpenView de Hewlett-Packard.

II. L'administration des réseaux informatiques

1. Définition

Le réseau est devenu une ressource indispensable au bon fonctionnement d'une organisation, une entreprise.

L'administration du réseau met en œuvre un ensemble de moyens pour :

- offrir aux utilisateurs un service de qualité,
- permettre l'évolution du système en incluant des nouvelles fonctionnalités,
- optimiser les performances des services pour les utilisateurs
- permettre une utilisation maximale des ressources pour un coût minimal.

Administration = partie opérationnelle d'un réseau

Les fonctions d'administration doivent permettre

- **l'extraction** des informations des éléments du réseau au moyen d'outils
  => récolte un grand nombre d'information,
- la **réduction** du volume d'information au moyen de filtres
  => Sélection d'information significative,
- le **stockage** des informations retenues dans une base de données d'administration,
- des **traitements** sur ces informations,
- offrir des **interfaces** (utilisateur d'administration, opérateur réseau).

2. L'organisation d'une administration

Qui a besoin d'administration et pour quoi faire ?

Il existe différents types de décision d'administration :

- **Décisions opérationnelles :** décision à court terme, concernant l'administration au jour le jour et opérations temps réel sur le système
- **Décisions tactiques :** décision à moyen terme concernant l'évolution du réseau et l'application des politiques de long terme
- **Décisions stratégiques :** décision de long terme concernant les stratégies pour le futur en exprimant les nouveaux besoins et désirs des utilisateurs.

Ces niveaux déterminent différents niveaux d'administration:

- **Le contrôle opérationnel réseau** pour les décisions opérationnelles
- **La gestion réseau** pour les décisions tactiques
- **L'analyse de réseau** pour les décisions tactiques et stratégiques
- **La planification** pour les décisions stratégiques

Conclusion

Dans ce chapitre, nous avons abordé des notions de base sur l'architecture d'un réseau local et les risques que ce dernier peut subir (vers, cheval de trois…). De ce fait, nous avons traité les différents moyens pour mieux protéger le réseau, et également l'administration d'un parc informatique, et les droits des utilisateurs

Le chapitre suivant décrira l'étude de l'existant de la société Marsa Maroc de Casablanca.

Chapitre 3

L'étude de l'existant

Le but de ce chapitre est l'étude du réseau existant de MARSA Maroc et d'y établir une vu d'ensemble sur les différents aspects physiques et logique de son parc informatique, à fin que nous puissions proposer des recommandations et solutions pour re-implémenter un réseau fiable, rapide, sécurisé et moins couteux.

I. Architecture du réseau informatique de l'existant

Le port Casablanca opère au premier port du Royaume pour les activités import et export. Marsa Maroc assure le traitement d'un trafic très diversifié dont le volume est de près de 15 millions de tonnes annuellement.

Cette diversité a nécessité la mise en place d'une organisation par pôle d'activité basée sur la spécialisation des infrastructures, des équipements et des ressources humaines et adaptée aux deux activités principales qui sont le conteneur et le roulier d'une part et le divers d'autre part.

MARSA Maroc offre au port de Casablanca les services logistique suivants :

- Services aux navires : lamanage
- Services à la marchandise : manutention, magasinage, transfert aux aires de stockage, pointage, pesage, chargement et déchargement de camions, location de matériel, empotage et dépotage des conteneurs et remorques
  Information en temps réel : le service MARSA Conteneur pour le suivi des conteneurs dans l'enceinte portuaire.
- Le réseau de la DEPC qui appartient au réseau MARSA Maroc est composé de trois principaux bloques:
  - **La connexion avec le siège qui permet de mutualiser les accès aux ressources qui existent sur les deux réseaux comme pour l'accès internet qui se fait depuis le siège social.**
  - **Le réseau local qui comporte les serveurs et les utilisateurs réparties sur les différents sites de la DEPC.**
  - **Les connexions avec les partenaires à savoir la douane et l'EDI.**

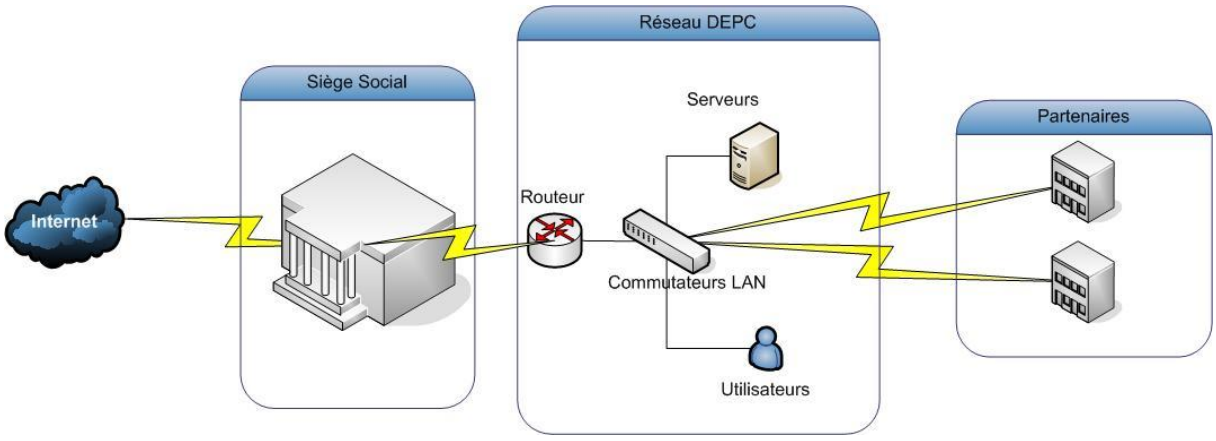


Figure 7 : Schéma de l'architecture Global DEPC

Dans le présent paragraphe nous allons détailler ces principaux bloques.

1. Le réseau local

Afin de connaitre toute information concernant l'architecture du réseau tel que l'adressage IP(1), les Neighbors et les interfaces de connexion, on a utilisé le protocole CDP.

1.1. Le protocole CDP

1.1.1. Introduction au protocole CDP

CDP (Cisco Discovery Protocol) est un protocole qui permet d'obtenir des informations sur les équipements voisins, comme leurs types, les interfaces du routeur auxquelles ils sont connectés, les interfaces utilisées pour établir les connexions, ainsi que leurs numéros de modèle.

Lors du démarrage d'un équipement Cisco, CDP démarre de façon automatique et permet à l'équipement de détecter les équipements voisins qui exécutent comme lui ce protocole.

Chaque équipement configuré pour CDP envoie périodiquement des messages, appelés annonces, aux équipements réseau directement connectés. Chaque équipement annonce au moins une adresse à laquelle il peut recevoir des messages SNMP(2) (Simple Network Management Protocol). Les annonces contiennent également des informations de « durée de vie » ou durée de conservation, indiquant pendant combien de temps les équipements récepteurs doivent conserver les informations CDP avant de les éliminer. De plus, chaque équipement écoute les messages CDP périodiques envoyés par les autres équipements afin d'identifier ceux qui se trouvent dans le voisinage.

1.1.2. Les informations obtenues avec CDP

CDP sert principalement à découvrir tous les équipements Cisco qui sont directement connectés à un équipement local. Exécutez la commande show cdp neighbors pour afficher les mises à jour CDP sur l'équipement local.

La figure illustre la façon dont le protocole CDP transmet à l'administrateur réseau les données recueillies. Tous les routeurs exécutant le protocole CDP partagent avec leurs voisins des informations protocolaires. L'administrateur réseau peut visualiser les résultats de cet échange d'informations via CDP sur une console reliée à un routeur local.

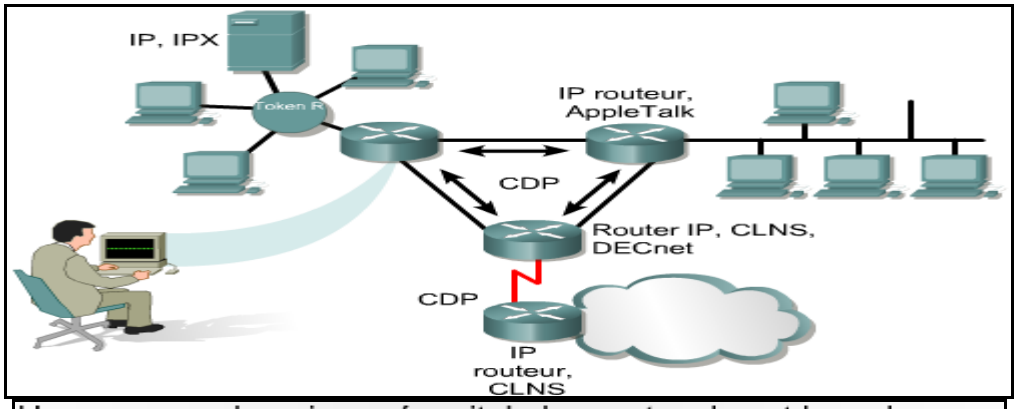


Figure 8: schéma présente la façon dont le CDP transmet les données à l'administrateur

L'administrateur utilise la commande show cdp neighbors pour afficher les informations sur les réseaux directement connectés au routeur. CDP fournit des informations sur chaque équipement CDP voisin en transmettant des TLV (Type Length Value), c'est-à-dire des blocs d'informations incorporés dans des annonces CDP.

Les TLV d'équipement affichées par les commandes **show cdp neighbors** sont notamment:

- L'identifiant,
- L'interface locale,
- La durée de conservation,
- La capacité,
- La plate-forme,
- L'ID du port.

Remarquez: Que le routeur situé au niveau le plus bas sur la figure n'est pas directement connecté au routeur de la console de l'administrateur.

Pour obtenir des informations CDP sur cet équipement, l'administrateur doit établir une session telnet[3] avec un routeur qui lui est directement connecté.

1.1.3. Création d'un schéma de réseau de l'environnement

Le CDP est un protocole simple ne surchargeant pas les réseaux. Une trame CDP peut être de petite taille mais fournir de nombreuses informations utiles sur les équipements Cisco voisins connectés. Ces informations peuvent être utilisées pour créer un schéma du réseau en utilisant le Telnet et la commande show CDP.

```
Rt2#show cdp neighbors
Capability Codes: R-Router, T-Trans Bridge, B-Source
Route Bridge, S-Switch, H-Host, I-IGMP, r-Repeater

DeviceID Local Intrfce Holdtme Capablty Platform  Port ID
Rt3      Ser0/1        152     R        2500      Ser1
Rt1      Ser0/0        121     R        2620      Ser0/0
Rt2#
```

1.2. Le schéma global

Le réseau local DEPC est composé de plusieurs commutateurs dont le nœud central est basé sur trois Switch fédérateurs 4507R reliés entre eux et qui sont à leurs tours connectés aux Switchs, serveurs, bridges…

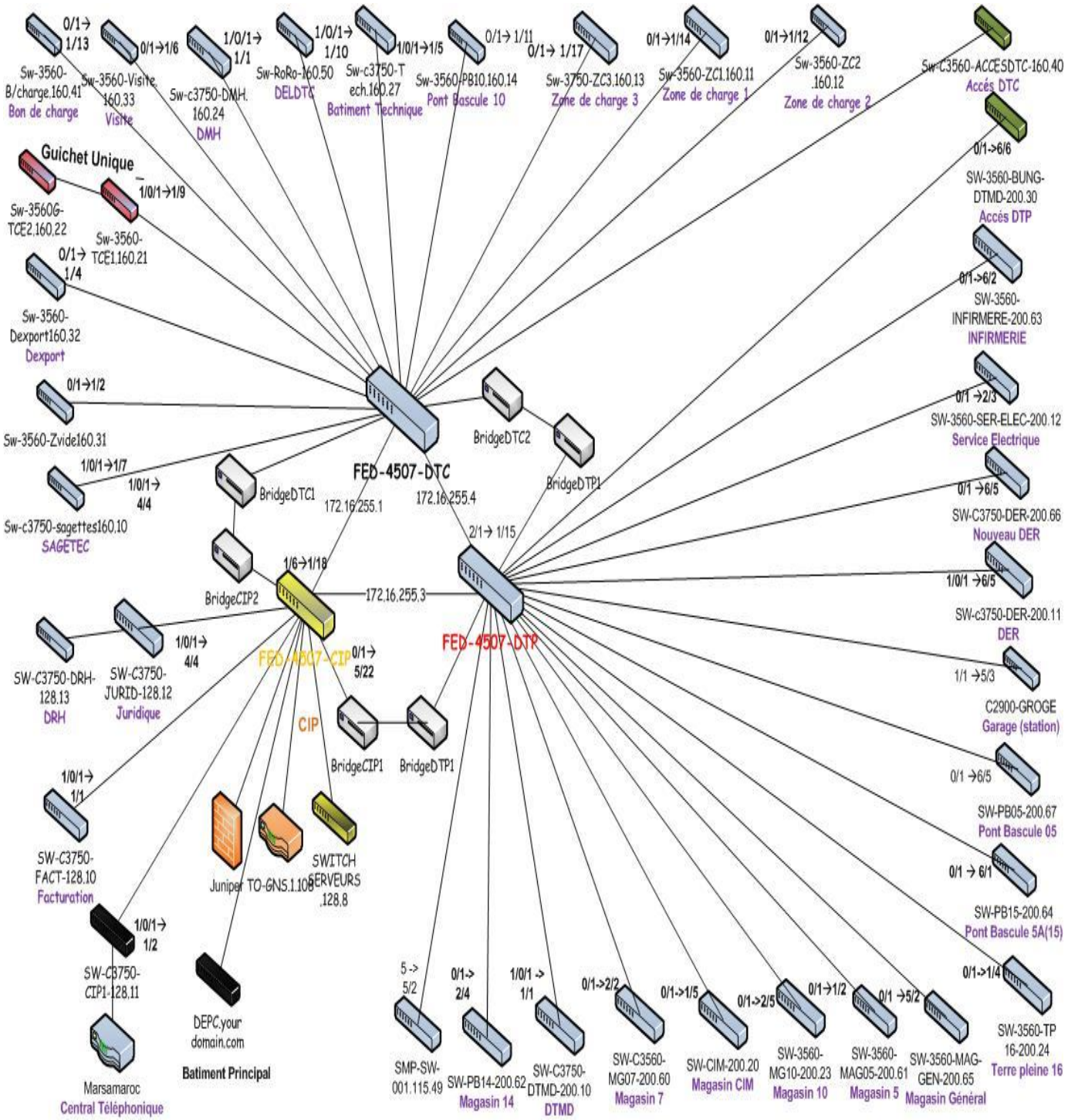


Figure 9 : Schéma du réseau LAN DEPC

L'adressage IP de chaque équipement ainsi que leur emplacement est décrit sur un tableau à l'annexe A (Tableau4).

D'après l'architecture obtenue ci-dessus, nous avons établis les voisins à chaque équipement de réseau. Voir annexe A (Tableau5).

1.3. La segmentation du réseau LAN de Marsa

1.3.1. Introduction aux VLANs

Un LAN virtuel (ou VLAN) est un domaine de broadcast créé par un ou plusieurs commutateurs. C'est un réseau local regroupant un ensemble de machines de façon logique et non physique.

En effet dans un réseau local, la communication entre les différentes machines est régie par l'architecture physique. Grâce aux réseaux virtuels (VLANs) il est possible de s'affranchir des limitations de l'architecture physique (contraintes géographiques, contraintes d'adressage, ...).

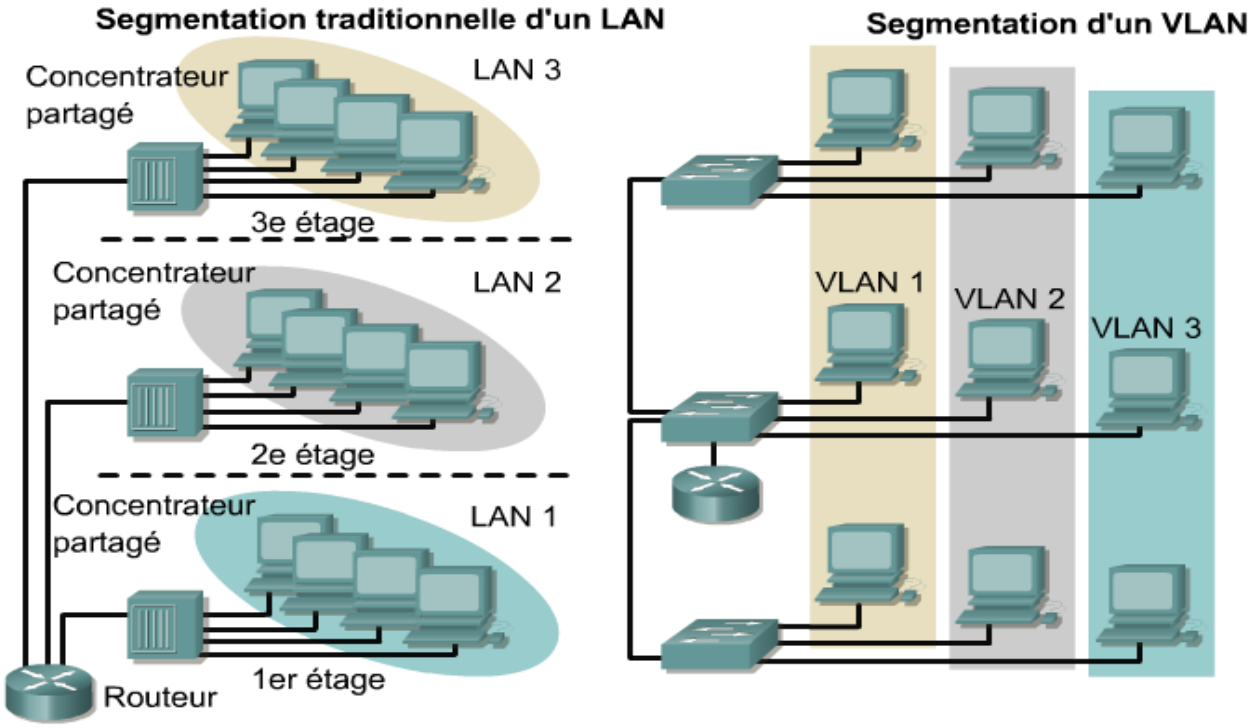


Figure 10 : schéma présente la segmentation de LAN et VLAN

1.3.2. Avantages des LAN virtuels (VLAN)

Le principal avantage des VLANs est qu'ils permettent à l'administrateur réseau d'organiser le LAN de manière logique et non physique. Cela signifie qu'un administrateur peut effectuer toutes les opérations suivantes:

- Déplacer facilement des stations de travail sur le LAN,
- Ajouter facilement des stations de travail au LAN,
- Modifier facilement la configuration LAN,
- Contrôler facilement le trafic réseau,
- Améliorer la sécurité.

1.3.3. L'adressage et VLANs

Le réseau utilisé pour l'adressage du réseau Marsa Maroc est 172.16.0.0/16. Ce réseau est segmenté selon le tableau suivant:

Segmentation du réseau LAN de Marsa Maroc								
Equipement	**Plage globale**	**N° VLAN**	**Nom VLAN**	**Adressage Data**	**Masque**	**Nombre d'IP**	**Pool d'adresse**	**Broadcast (5)**
			inter-switch	172.16.255.0	255.255.255.0	254	172.16.255.1-172.16.255.254	172.16.255.255
FED-4507R-CIP	172.16.128.0/19	1	**Ancien**	172.16.0.0	255.255.240.0	4094	172.16.0.1 to 172.16.15.254	172.16.15.255
		20	**Admin**	172.16.128.0	255.255.255.128	126	172.16.128.1 to 172.16.128.127	172.16.128.127
		2	**Interco-WAN**	172.16.128.128	255.255.255.128	126	172.16.128.129 to 172.16.128.254	172.16.128.254
		3	**Serveur-prod**	172.16.130.0	255.255.255.0	254	172.16.130.1 to 172.16.130.254	172.16.130.255
		4	**Users**	172.16.132.0	255.255.254.0	510	172.16.132.1 to 172.16.133.254	172.16.133.255
		5	**Voice**	172.16.134.0	255.255.254.0	510	172.16.134.1 to 172.16.135.254	172.16.135.255
		6	**Pesage**	172.16.136.0	255.255.255.0	254	172.16.135.1 to 172.16.135.254	172.16.135.255
		7	**P-Affichage**	172.16.137.0	255.255.255.0	254	172.16.136.1 to 172.16.137.254	172.16.136.255
		21	**VTS**	172.16.138.0	255.255.255.0	254	172.16.137.1 to 172.16.137.254	172.16.137.255
		22	**SOMAPOR**	172.16.139.0	255.255.255.0	254	172.16.138.1 to 172.16.138.254	172.16.138.255
		23	**Douane**	10.1.1.0	255.255.255.252	2	10.1.1.1 to 10.1.1.2	10.1.1.3
		24	**ANP**	10.255.255.0	255.255.255.252	2	10.255.255.1 to 10.255.255.2	10.255.255.3
FED-4507R-DTC	172.16.160.0/19	20	**Admin**	172.16.160.0	255.255.255.128	126	172.16.160.1 to 172.16.160.126	172.16.160.127
		4	**Users**	172.16.162.0	255.255.254.0	510	172.16.162.1 to 172.16.163.254	172.16.163.255
		5	**Voice**	172.16.164.0	255.255.254.0	510	172.16.164.1 to 172.16.165.254	172.16.165.255
		8	**Pesage**	172.16.166.0	255.255.255.0	254	172.16.166.1 to 172.16.166.254	172.16.166.255
		10	**P-Affichage**	172.16.167.0	255.255.255.0	254	172.16.167.1 to 172.16.167.254	172.16.167.255
		22	**VTS**	172.16.168.0	255.255.255.0	254	172.16.168.1 to 172.16.168.254	172.16.168.255
FED-4507R-DTP	172.16.192.0/19	20	**Admin**	172.16.200.0	255.255.255.128	126	172.16.200.1 to 172.16.200.126	172.16.200.127
		4	**Users**	172.16.192.0	255.255.254.0	510	172.16.192.1 to 172.16.193.254	172.16.193.255
		5	**Voice**	172.16.194.0	255.255.254.0	510	172.16.194.1 to 172.16.195.254	172.16.195.255
		8	**Pesage**	172.16.196.0	255.255.255.0	254	172.16.196.1 to 172.16.196.254	172.16.196.255
		9	**P-Affichage**	172.16.197.0	255.255.255.0	254	172.16.197.1 to 172.16.197.254	172.16.197.255
		21	**SOMAPOR**	172.16.199.0	255.255.255.0	254	172.16.199.1 to 172.16.199.254	172.16.199.255

Tableau 1 : Tableau détaillé d'adressage des VLAN

1.4. Les serveurs DEPC

Le tableau suivant résume l'ensemble des serveurs(6) déclarés par la DEPC ainsi que leurs emplacements sur les Switch(4):

Serveurs	Adresse IP	Base de données	Switch	Port	VLAN
Hraccess	172.16.2.170	*****	FED-4507R-CIP	Gi5/14	SRV-prod
Boserver	172.16.1.241	SQL SERVER 2000	FED-4507R-CIP	Gi5/14	SRV-prod
apipro	172.16.1.2	SQL SERVER 2000	FED-4507R-CIP	Gi5/14	SRV-prod
Syfcom	172.16.3.161	*******	FED-4507R-CIP	Gi5/14	SRV-prod
Pesage	172.16.12.251	SQL BASE	Switch-Serveurs	Gi0/23	Pesage
Pesage Backup	172.16.12.252	SQL BASE	Switch-Serveurs	Gi0/24	Pesage
Nouveau Serveur Pesage	172.16.1.105	DB2	Switch-Serveurs		Pesage
Extranet	172.16.1.106	********	Switch-Serveurs	Gi0/9	SRV-prod
Syfcom Reporting	172.16.3.162		FED-4507R-CIP	Gi5/14	SRV-prod
Exchange	172.16.3.20		Switch-Serveurs	Gi0/5	SRV-prod

Tableau 2: Tableau des serveurs

1.4.1. Utilisation des ports des Switchs DEPC

La commande suivante affiche l'état des ports sur un switch cisco:

switch# show interfaces status

Port	Name	Status	Vlan	Duplex	Speed	Type
Fa1/0/1		notconnect	2	auto	auto	10/100BaseTX
Fa1/0/2		notconnect	2	auto	auto	10/100BaseTX
Fa1/0/3		connected	2	a-full	a-100	10/100BaseTX
Fa1/0/4		connected	4	a-full	a-100	10/100BaseTX
Fa1/0/5		connected	2	a-full	a-100	10/100BaseTX
Fa1/0/6		connected	10	a-full	a-100	10/100BaseTX
Fa1/0/7		connected	2	a-full	a-100	10/100BaseTX

Le tableau suivant résume l'utilisation des ports des différents équipements de la DEPC :

Device Name	Nombres de Ports	Ports Connectés	Ports Libres
FED-4507R-CIP.sodep.co.ma	101	40	61
SW-C3750-FACT-128.10.sodep.co.ma	52	22	29
SW-C3750-CIP1-128.11.sodep.co.ma	104	54	50

SW-C3750-JURID-128.12.sodep.co.ma	26	24	2
SW-C3750-DRH-128.13.sodep.co.ma	26	12	14
Switch-Serveurs	28	13	15
FED-4507R-DTC.sodep.co.ma	68	29	39
SW-C3750-SAGETES-160.10.sodep.co.ma	52	16	36
SW-3560-ZC1-160.11.sodep.co.ma	9	3	6
SW-3560-ZC2-160.12	9	6	3
SW-3560-ZC3-160.13.sodep.co.ma	9	3	6
SW-3560-TCE1-160.21	52	31	21
SW-3560G-TCE2.160.22	28	19	9
SW-C3750-DMH-160.24.sodep.co.ma	26	9	17
SW-C3750-TECH-160.27.sodep.co.ma	26	3	23
SW-C3560-ZVIDE-160.31	9	7	2
SW-3560-Dexport-160.32.sodep.co.ma	9	3	6
SW-3560-Visite-160.33.sodep.co.ma	9	2	7
SW-C3560-ACCESDTC-160.40.sodep.co.ma	9	9	0
SW-3560-B/Charge.sodep.co.ma	9	4	5
SW-RORO-160.50	26	8	18
FED-4507R-DTP.sodep.co.ma	66	36	30
SW-C3750-DTMD-200.10.sodep.co.ma	52	17	35
SW-C3750-DER-200.11.sodep.co.ma	26	9	17
SW-3560-SER-ELEC-200.12.sodep.co.ma	9	3	6
SW-CIM-200.20	9	7	2
SW-3560-MG10-200.23.sodep.co.ma	9	6	3
SW-3560-TP16-200.24.sodep.co.ma	9	2	7
SW-3560-Bung-DTMD-200.30.sodep.co.ma	9	7	2
SW-C3560-MG07-200.60.sodep.co.ma	9	3	6
SW-3560-Mag05-200.61.sodep.co.ma	9	3	6
SW-PB14-200.62	9	3	6
SW-3560-INFIRMERIE-200.63.sodep.co.ma	9	4	5
SW-PB15-200.64.sodep.co.ma	9	3	6
SW-3560-Mag-Gen-200.65.sodep.co.ma	9	3	6
SW-C3750-DER-200.66	52	14	38
SW-C3750-DER-200.66	52	14	38

Tableau 3 : Utilisation des ports des Switchs DEPC

2. Connexion avec la Douane

La douane est l'un des principaux partenaires connectés au réseau DEPC; le but de cette interconnexion est de permettre aux utilisateurs de la douane d'accéder au serveur AS400 de la DEPC.

Cette connexion est assurée par une liaison FO[(7)] sécurisée par deux firewalls[(8)] Juniper SSG140 des deux côtés selon le schéma suivant:

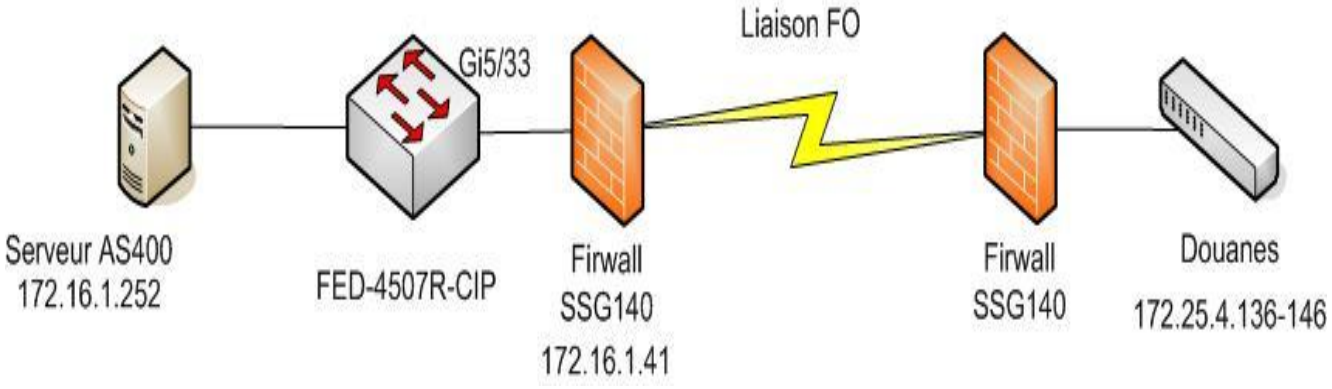


Figure 11 : Schéma de Connexion DEPC-Douanes

3. Connexion avec l'EDI

La connexion avec la société d'Echange de Données Informatisée EDI se fait par l'intermédiaire d'une liaison LS assurée par une Routeur[9] Cisco 1600 selon le schéma suivant:

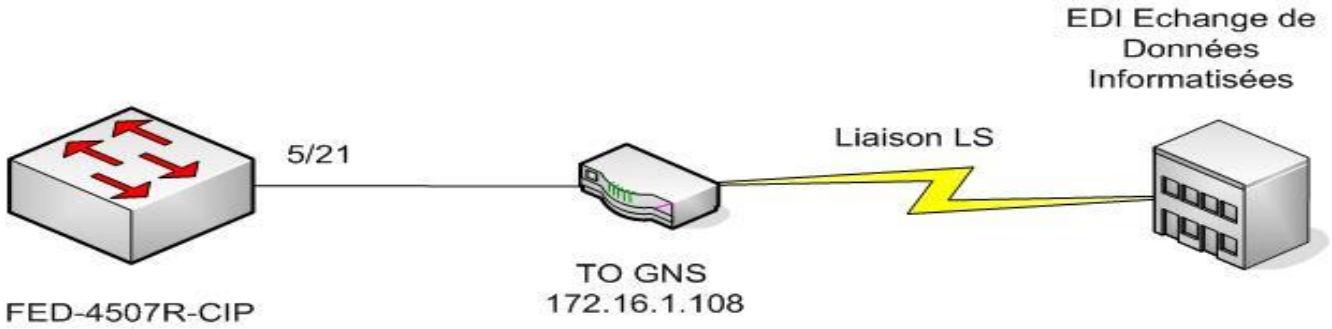


Figure 12 : Schéma de Connexion DEPC-EDI

4. Connexion avec le siège

La connexion entre la DEPC et le siège social est une liaison FH[10] assurée par un routeur Cisco relié au Switch de commutation du deuxième étage et d'un Juniper WX 500 qui assure l'accélération du flux entre les deux sites :

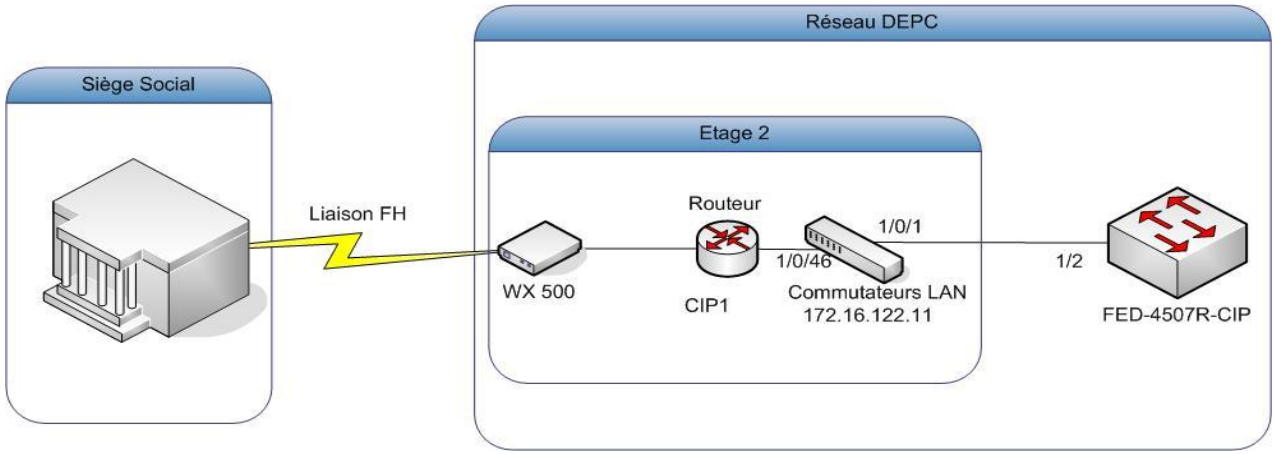


Figure 13 : Schéma de Connexion DEPC-Siège

II. Analyse critique de l'existant

L'analyse de réseau et sécurité a pour axes prioritaires de faire un état des lieux précis de l'infrastructure réseau, et de mettre en exergue l'ensemble des failles fonctionnelles et techniques mettant en danger le système d'information de la société.

L'analyse de l'existant sera divisée en deux principaux volés :

1. L'architecture du réseau DEPC

L'architecture du réseau DEPC comme expliqué dans la partie précédente est structurée autour de trois fédérateurs(11) centraux sur lesquels sont connectés les Switchs(4) d'accès des utilisateurs.

Dans cette architecture, il y a plusieurs points à améliorer dont on peut citer:

- **Le problème de disponibilité des fédérateurs,**
- **Le site CIP est le plus critique, tel qu'il assure l'interconnexion du DEPC avec l'ensemble des services: Internet, Siège, Partenaires, Serveurs…**
- **Le problème de débit de connexion au siège suite à la forte utilisation d'internet ce qui provoque des ralentissements et des temps de réponse très lent.**
- **La nécessité de mettre en place un site de secours.**

2. La sécurité du réseau DEPC

Lors de nos visites sur site nous avons noté plusieurs failles de sécurité :

- **L'utilisation de la connexion 3G en même temps que l'accès au réseau local risque d'infecté ce dernier.**
- **Le personnels et les utilisateurs provisoire du DEPC possèdent les droits administrateurs ce qui leur permet d'avoir le contrôle total sur leur station de travail, cela présente un grand risque pour la sécurité du réseau.**
- **Mauvaise utilisation de l'antivirus (non installé, désactivé ou non mis à jours).**
- **La connexion avec l'EDI est complètement non sécurisée: cette connexion est seulement basée sur un routeur directement connecté sur le LAN (le fédérateur).**
- **Pas de logiciels pour la gestion des logs des Switchs et différents équipements.**
- **La configuration du SNMP(2) sur les Switch n'est pas sécurisée suite à un problème de version.**

- **L'accès aux différents équipements est complètement non sécurisé: Accès Telenet seulement, même loging/PWD pour tous les équipements, pas d'accès liste pour le contrôle d'accès depuis les postes d'administration.**

- **Pas de contrôle d'accès entre les différents VLAN; pas d'accès listes appliquées.**

- **Les serveurs ne sont pas protégés des accès non autorisés.**

Conclusion

Dans ce chapitre, nous avons présenté l'état actuel du parc informatique de la société Marsa Maroc et les différentes problématiques.

Dans le chapitre qui suit, nous proposeront des recommandations pour avoir une architecture optimale et plus sécurisé.

Chapitre 4

Les recommandations

Dans ce chapitre nous présentons un ensemble de recommandations et solutions à mettre en place pour mieux gérer et sécurisé le réseau de Marsa Maroc.

I. L'architecture du réseau DEPC

Pour répondre aux différentes problématiques susmentionnées tout en gardant les acquis positifs du réseau actuel et en exploitant au mieux ces fonctionnalités avec le moindre cout.

1. La redondance des Switchs Fédérateurs

Sur le réseau de la DEPC les trois Switch Fédérateurs sont réparties sur trois bâtiments géographiquement éloignés, ils sont reliés entre eux par des liaisons Fibres Optique backupés par une liaison sans fil.

Ces Switchs sont instantanément confronté à des problèmes d'envergure grave sur le système informatique. A titre d'exemple:

- **Une panne matérielle des Switchs (duré de vie dépassée),**
- **Une coupure électrique,**
- **Une catastrophe naturelle (incendie, inondation…).**

La redondance se limite au fédérateur principal CIP en mettant un second fédérateur de secours qui se réplique en permanence avec le fédérateur CIP et sont en partage de charge.

En pratique, il faut installer un deuxième fédérateur principal sur un site éloigné à fin d'éviter qu'un éventuel problème sur site impacte la totalité du réseau et bloque le système informatique de Marsa Maroc.

Lorsqu'un fédérateur tombe en panne, le flux réseau sera basculé sur le fédérateur de secours en attendant la réparation du matériel posant problème.

Concernant les autres fédérateurs DTC et DTP, nous n'avons pas besoin d'avoir une duplication identique du matériel (en raison de coût). En revanche nous proposons de mettre en place des Switchs pour assurer la transmission de données en cas de panne de l'un de ces fédérateur, et aussi nous proposons d'installé une liaison sans fils permettant une réplication mutuelle et permanente entre les fédérateurs.

Le schéma ci-dessous nous montre l'architecture susmentionnée.

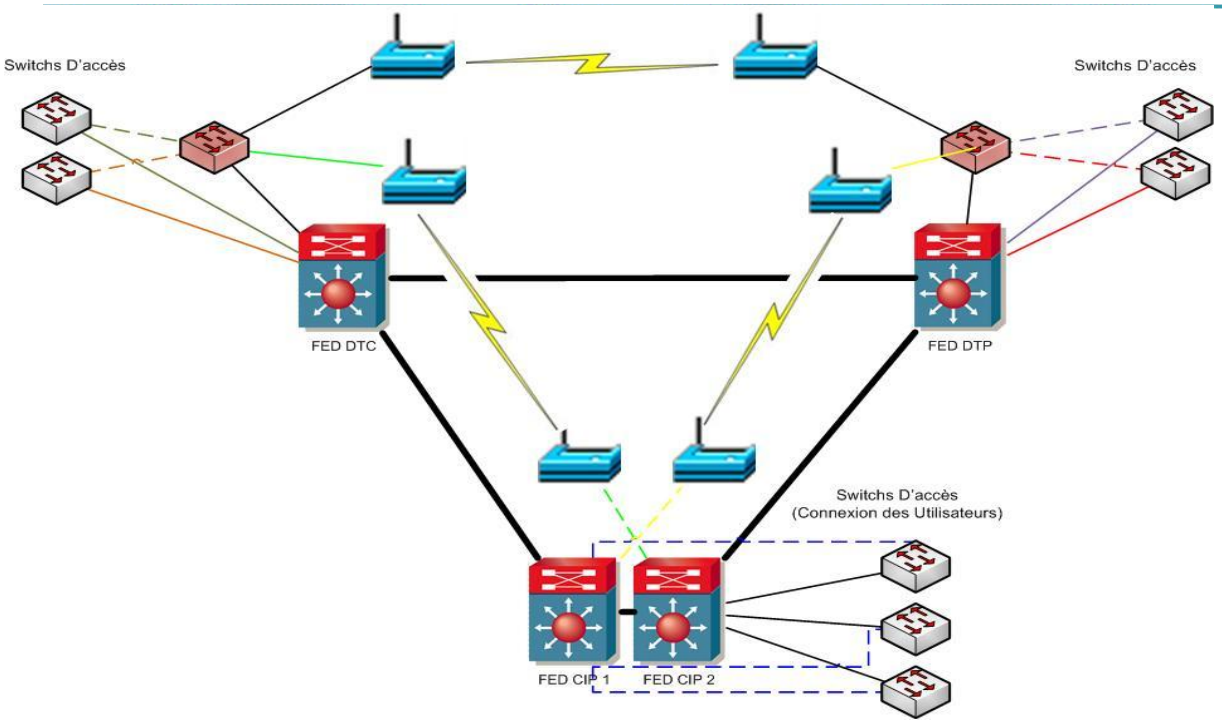


Figure 14 : Schéma de Redondance Variante 1 : Sans Fil

Remarque: Il faut avoir 2 liaisons entre les sites CIP.

L'ensemble des fédérateurs CIP (principale et de secours) forment un seul réseau et la liaison entre eux doit avoir une bande passante importante à fin d'assurer la transmission du flux sur cette liaison.

Les liaisons entre les commutateurs fédérateurs et les équipements d'étage peuvent être réalisées en cuivre ou en fibre optique, le choix dépendant de la distance.

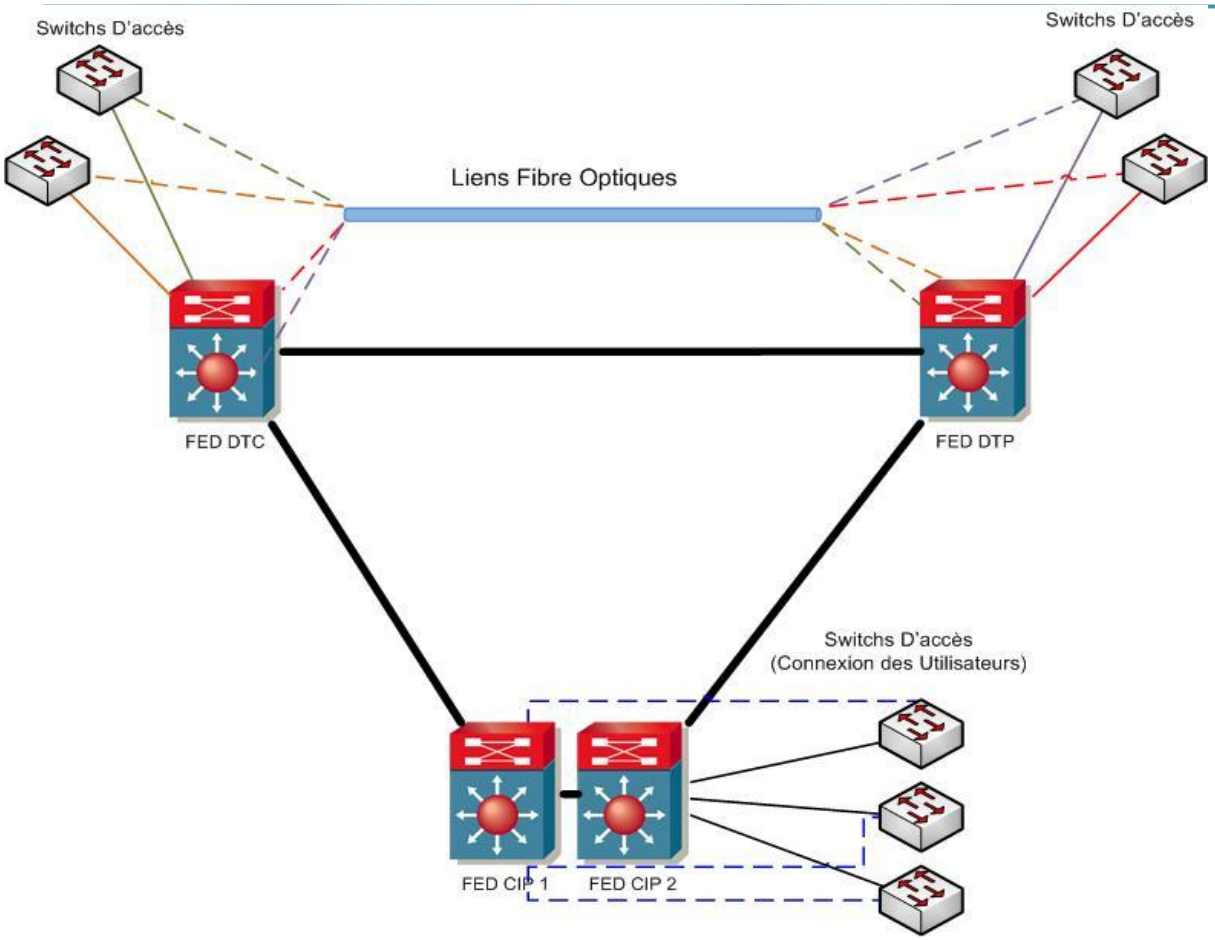


Figure 15: Schéma de Redondance Variante 2 : Fibre Optique

2. Une Architecture Modulaire

Afin d'assurer une interconnexion sécurisée et évolutive entre les différents services de la DEPC, nous avons proposé de segmenter le réseau selon chaque service, et aussi pour mieux séparer les utilisateurs étrangers à l'accès aux machines strictement à usage privé.

Pour que les machines seront placées sur un segment du réseau ouvert aux accès en provenance de l'extérieur, mais relativement isolé du réseau intérieur, afin qu'un visiteur étranger à l'entreprise ne puisse pas accéder aux machines à usage strictement privé. Les DMZ (zone démilitarisée) nous permettent de réaliser la segmentation du réseau.

Nous proposons l'installation d'un Firewall central redondé sur lequel sont branchées comme DMZ les zones Datacenter, téléphonie, Point d'accès Internet et Partenaires. Chacune des zones présente une utilité fonctionnelle à part qui peut évoluer et se développer indépendamment des autres blocks:

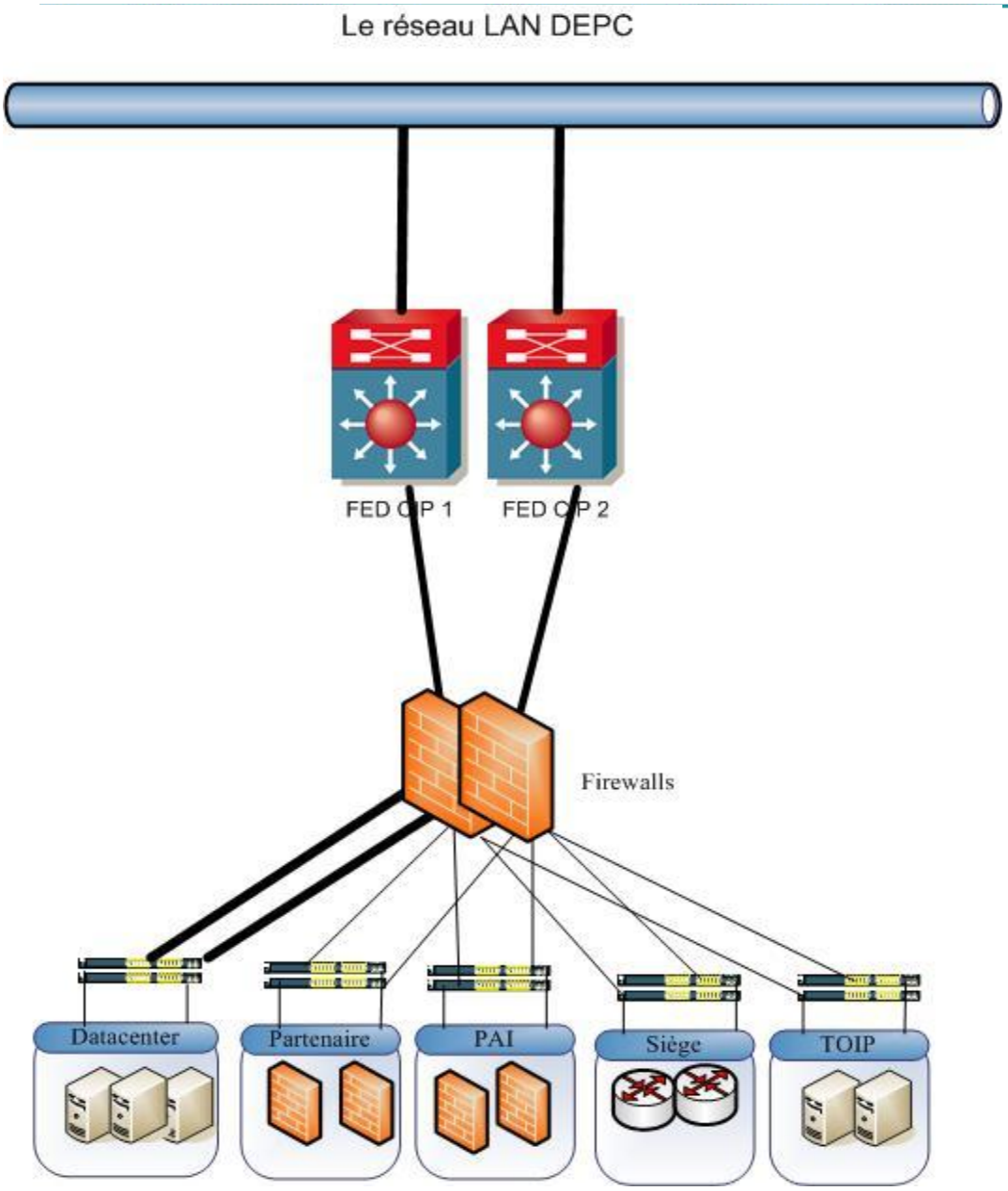


Figure 16: Architecture Réseau Modulaire

Pour chaque plateforme de cette architecture nous vous proposons ce qui suit :

- **Le Datacenter : hébergera les serveurs DEPC, sera basée sur des Switchs Cisco Nexus(15) connectée au Firewall par des liens 10G.**

- **Partenaires : Pour l'interconnexion avec les différents partenaires DEPC ; pour cette zone on pourra adopter pour chaque Partenaire un Firewall indépendant ou utiliser le Firewall SSG existant pour cette interconnexion.**

- **PAI : le Point d'accès Internet, créer une sortie internet indépendante du siège pour contourner les lenteurs existants qui pousse les utilisateurs à**

utiliser des connexions 3G. Cette plateforme sera composer par des firewalls et outils de filtrage URL et Antivirus.

- **Siège : Pour la connexion avec le siège et se protéger mutuellement des propagations de virus des deux sens.**

- **TOIP : Pour créer une plateforme sécurisée de la téléphonie IP qui doit être isolée du LAN.**

3. Site de secours

Nous vous proposons de créer un site de secoure sur le site DTC qui permettra de backuper les plateformes existants sur le site principal CIP, cette plateforme de secours sera directement liée au Firewall central pour qu'elle soit complètement indépendante du réseau des Utilisateurs :

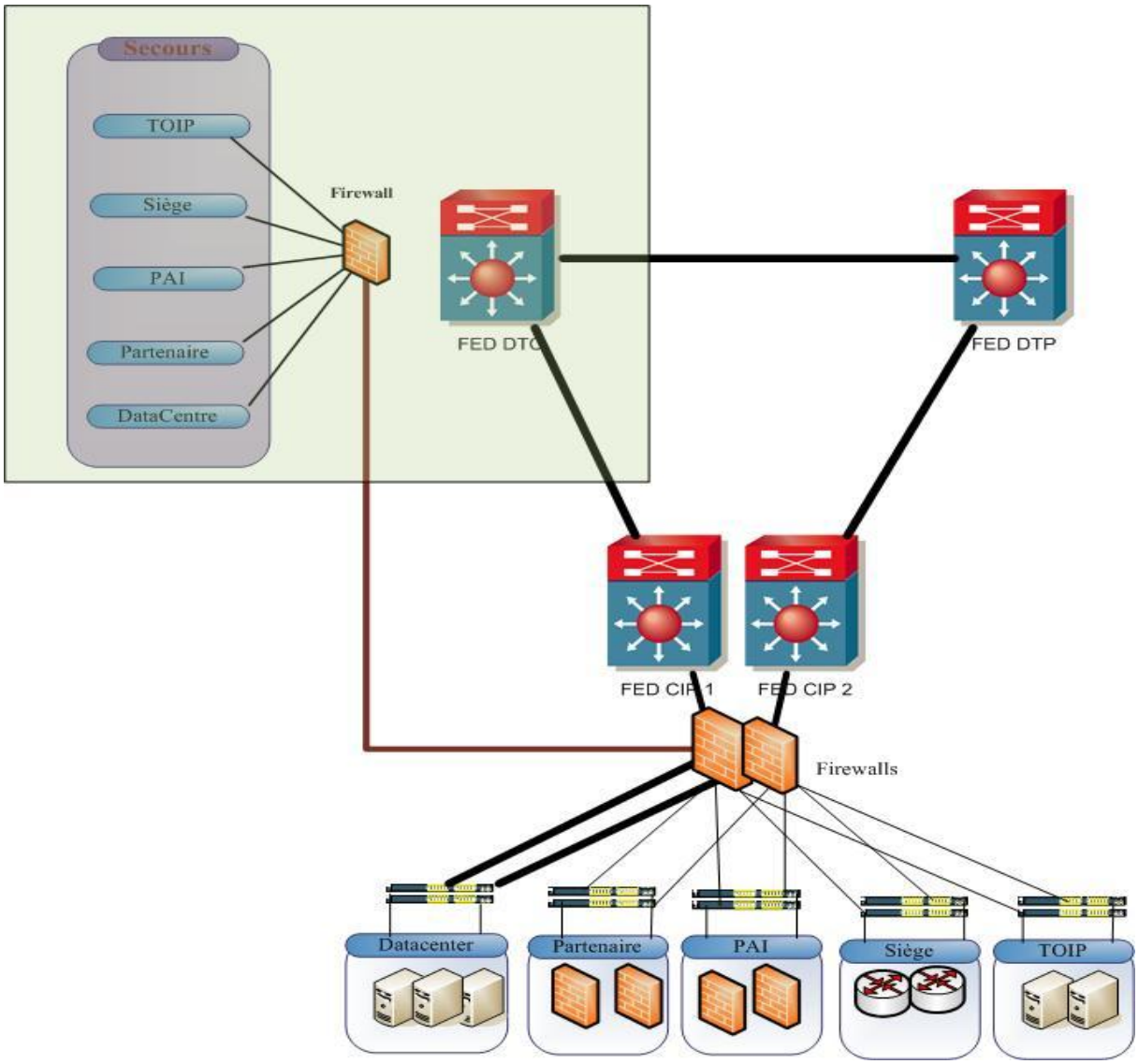


Figure 17 : Architecture Site de secours

II. Recommandations sécurité

Pour répondre aux différentes failles de sécurité que nous avons relevée dans les paragraphes précédents nous vous recommandons ce qui suit :

- **Administration du domaine MARSA Maroc : Installation d'un serveur 2003 ou 2008 et configurer le contrôleur de domaine Active Directory pour gérer les utilisateurs (authentification lors de la connexion d'un profil, droit utilisateurs, gestion des groupes…)**

- **Mise en place d'une solution de contrôle d'accès au réseau DEPC (NAC).**

- **Mettre en place une infrastructure sécurisée pour les accès des partenaires.**

- **Activer le login sur les différents équipements et mettre en place une solution de gestion et de corrélation des logs qui permet une visualisation en temps réal des menaces.**

- **Mettre en place les best-practices de configuration de la SNMP [(2)].**

- **Mettre en place une solution firewall/IPS[(16)] qui permet de faire le contrôle nécessaire entre les différents VLAN.**

- **Mettre en place une solution Datacenter pour garantir un accès sécurisé et rapide aux serveurs.**

Les points cités en haut sont détaillés dans les paragraphes suivants :

1. L'administration du domaine Marsa

Lors de nos visites fréquentes sur le site informatique MARSA Maroc, nous avons constaté plusieurs failles au niveau de l'administration du réseau. En effet, tous les utilisateurs possèdent des droits administrateur sur leurs stations de travail et particulièrement sur les serveurs centraux. De ce fait l'administration du domaine n'est pas centralisée sur une seule personne.

Pour répondre à cette problématique, nous avons proposé d'installer un serveur principal 2003/2008 et y configurer l'Active Directory (A.D) pour mieux gérer les utilisateurs, contrôler l'accès aux données informatiques de MARSA Maroc et centraliser l'administration.

Dans l'Active Directory, l'administrateur du domaine peut créer des comptes utilisateurs et leurs applique des GPO (Groupe Policy Objet) permettant de restreindre les droits utilisateur, comme par exemple :

- **Supprimer la commande exécutée du menu démarrer,**

- **Désactiver le panneau de configuration.**

Ces restrictions serons appliquées sur le profil créé par l'administrateur et non pas sur le profil local de l'utilisateur.

2. Sécurisation du MAN de Marsa Maroc

Dans cette partie on présente la mise à niveau du réseau local du Marsa Maroc par le déploiement d'une nouvelle technologie de contrôle NAC (Network Admission Control).

Lors de nos visites sur site nous avons rencontrés les problèmes suivants :

- **Antivirus non installé, désactiver ou non mis à jour sur certains poste utilisateurs.**
- **Systèmes d'exploitation non mis à jours.**
- **Des utilisateurs non identifiés et qui peuvent accéder au réseau.**

La mise en place d'une solution de contrôle d'accès au réseau DEPC permet de résoudre tous ces problèmes cités précédemment, et de rendre le réseau capable de se défendre tout seul.

De ce fait, la technologie NAC permet d'appliquer des politiques de correctifs sur les logiciels installés aux PC des utilisateurs et de rediriger les hôtes infectés ou non conforme à la politique vers des zones de quarantaines isolé du réseau de confiance. On trouve dans cette zone de quarantaine un serveur de mise à jour (antivirus, patchs) capable de remettre la machine à niveau avant de pouvoir autoriser l'accès au réseau.

2.1 définition

Cisco NAC (Network Admission Control) est un protocole proposé par Cisco, s'interpose entre les menaces évoluées et le réseau, c'est au moment où la machine demande l'accès au réseau qu'il convient de faire le contrôle.

2.2 Description générale de Cisco NAC

Les dégâts générés par les virus ont montré dans toute sa réalité l'inadéquation des dispositifs actuels de sécurité.

Cisco NAC offre une nouvelle solution complète qui permet aux organisations d'appliquer des politiques de correctifs logiciels sur les hôtes et de rediriger les systèmes non conformes et potentiellement vulnérables vers des environnements de quarantaine disposant de peu, voire d'aucun, accès au réseau.

En associant les informations sur l'état de la sécurité des points d'extrémité avec les conditions d'admission au réseau, Cisco NAC permet aux organisations d'améliorer de manière considérable la sécurité de leurs infrastructures informatiques.

Cisco NAC accorde l'accès au réseau de confiance des unités d'extrémité (PC, serveur) conforme et refuse les unités non conformes.

La décision d'accorder cet accès peut reposer sur des informations comme l'état du logiciel anti-virus du point d'extrémité ou la version du correctif de son système d'exploitation.

2.3 Les composants de technologie Cisco NAC

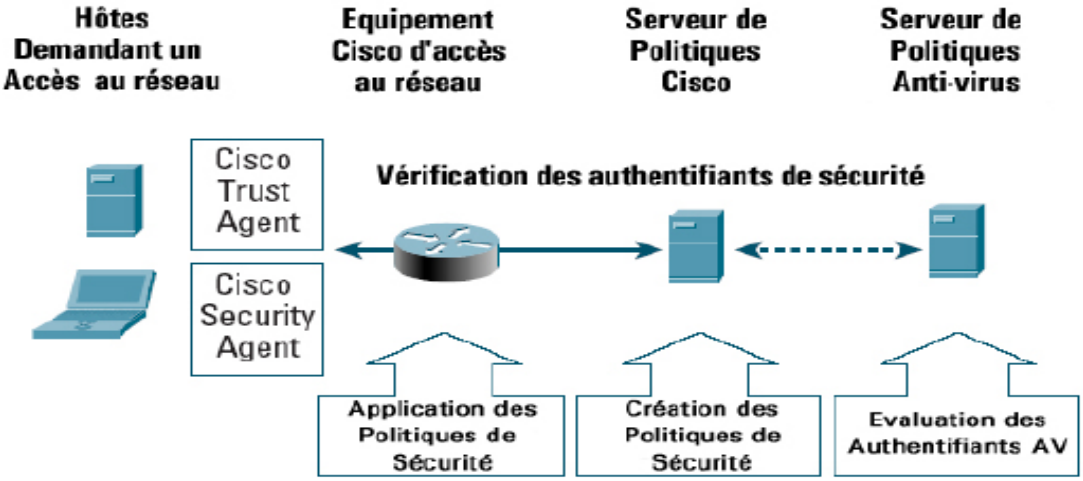


Figure 18 : Cisco NAC

Cisco NAC dispose des composants suivants :

- **Cisco Trust Agent (CTA) : Ce logiciel qui réside sur un système d'extrémité, collecte les informations sur l'état de l'unité provenant de nombreux clients logiciels de sécurité (client anti-virus, par exemple) et communique ces informations aux unités Cisco d'accès réseau chargées d'appliquer les contrôles d'admission.**

Cisco a fourni des licences de sa technologie CTA à ses partenaire anti-virus afin qu'ils puissent l'intégrée à Cisco Security Agent pour faire appliquer les privilèges d'accès en fonction de la version du correctif du système d'exploitation du point d'extrémité.

Cisco Security Agent, solution logicielle de protection de l'hôte dés le premier jour, évaluera la version, les correctifs et les informations de dépannage à chaud du système d'exploitation avant de les communiquer à Cisco trust agent.

Les hôtes qui ne disposent pas des correctifs requis peuvent ne recevoir qu'un accès limité au réseau, et même en être exclus.

- **Unités d'accès réseau : les routeurs, les commutateurs, les points d'accès sans fil et les serveurs de sécurité dédiés appliquent la politique de contrôle d'admission au réseau. Ces unités exigent des « authentifiants » de sécurité hôte et relaient l'information aux serveurs de politique qui prennent les décisions de contrôle d'admission au réseau.**

Selon la politique définie par l'utilisateur, le réseau applique la décision appropriée de contrôle d'admission (Autorisation, refus, quarantaine ou accès restreint).

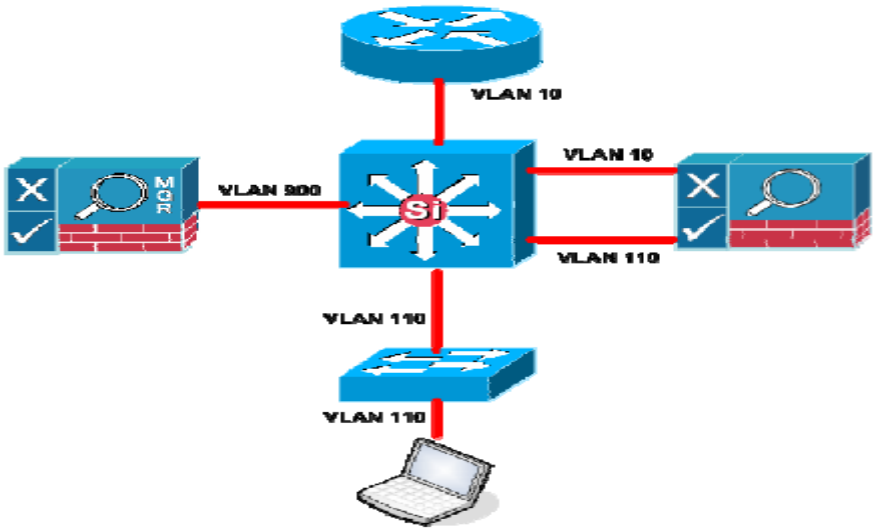
- **Serveur de politiques (Clean Access Server) : Ce serveur évalue les informations de sécurité du point d'extrémité provenant des unités d'accès au réseau et détermine la politique d'accès qu'il convient de lui appliquer.**

- **Système d'administration (Clean Access Manager) : console Web centralisée pour l'établissement des rôles, des contrôles, des règles et des politiques.**

Serveurs NAC ont deux modèles de déploiement de flux de trafic :

2.3.1 In Band

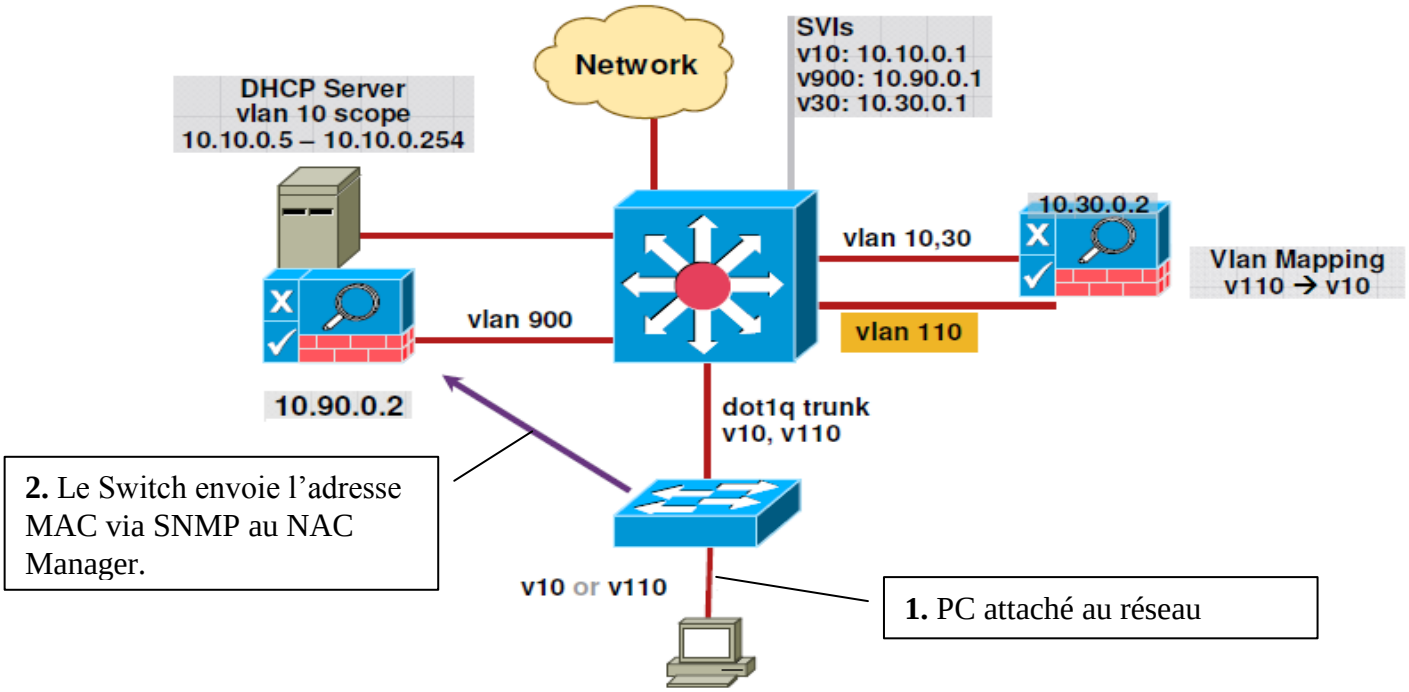
- Option de déploiement la plus facile,
- NAC Server est en ligne (dans le chemin de données) avant et après l'évaluation,
- ACL de filtrage et de limitation de bande passante.



2.3.2 Out Of Band

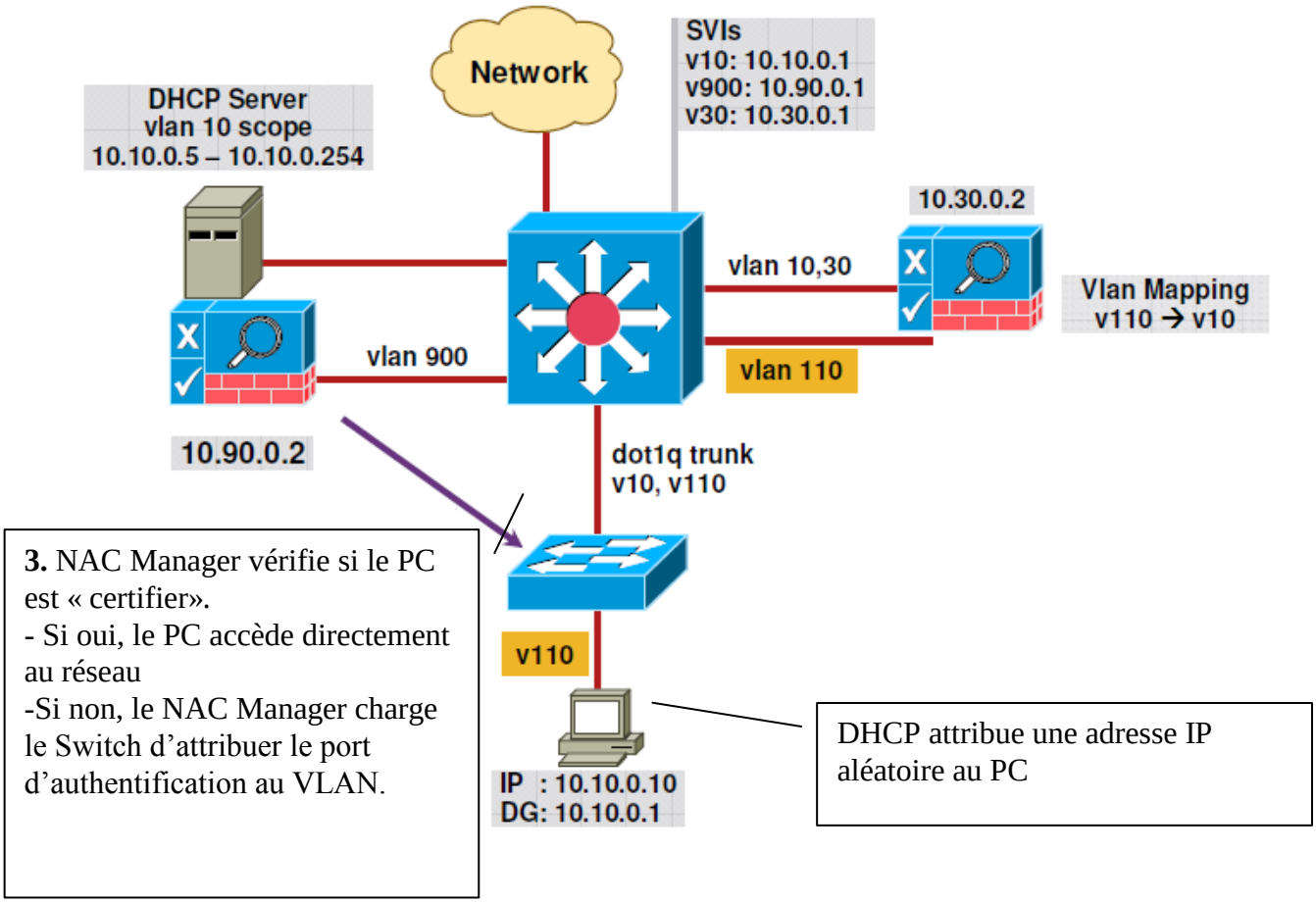
- NAC server est en ligne pour seulement l'évaluation,
- Basé sur le port VLAN et le rôle de contrôle d'accès,
- Le filtrage ACL et limitation de la bande passante pour l'évaluation.

➔ **Le processus de Flux de Out Of Band :**



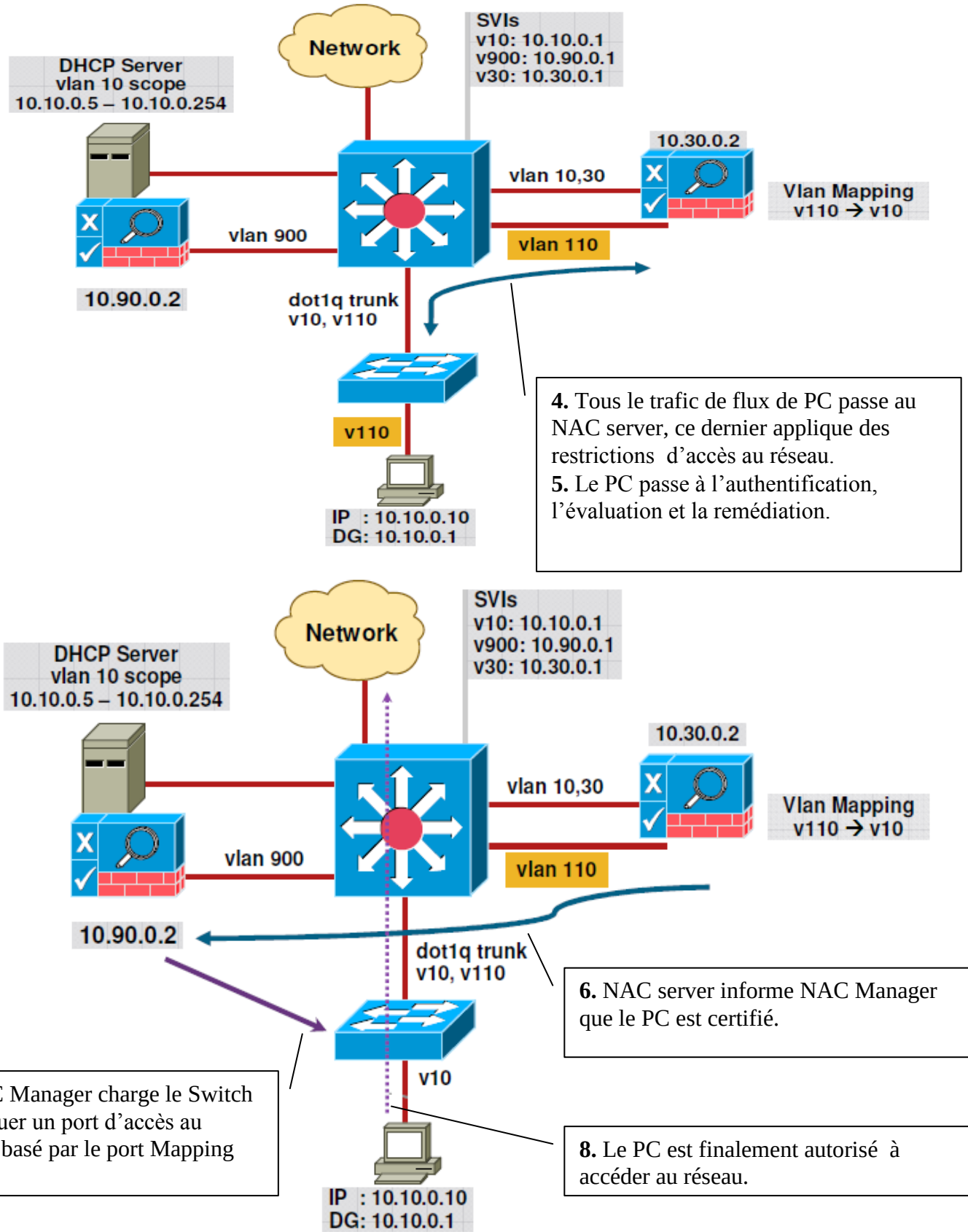
2. Le Switch envoie l'adresse MAC via SNMP au NAC Manager.

1. PC attaché au réseau



3. NAC Manager vérifie si le PC est « certifier».
- Si oui, le PC accède directement au réseau
-Si non, le NAC Manager charge le Switch d'attribuer le port d'authentification au VLAN.

DHCP attribue une adresse IP aléatoire au PC



2.4 La mise en place de la technologie NAC au réseau de Marsa Maroc

D'après l'architecture détaillée en haut de la technologie NAC, nous avons proposé l'architecture du réseau suivant :

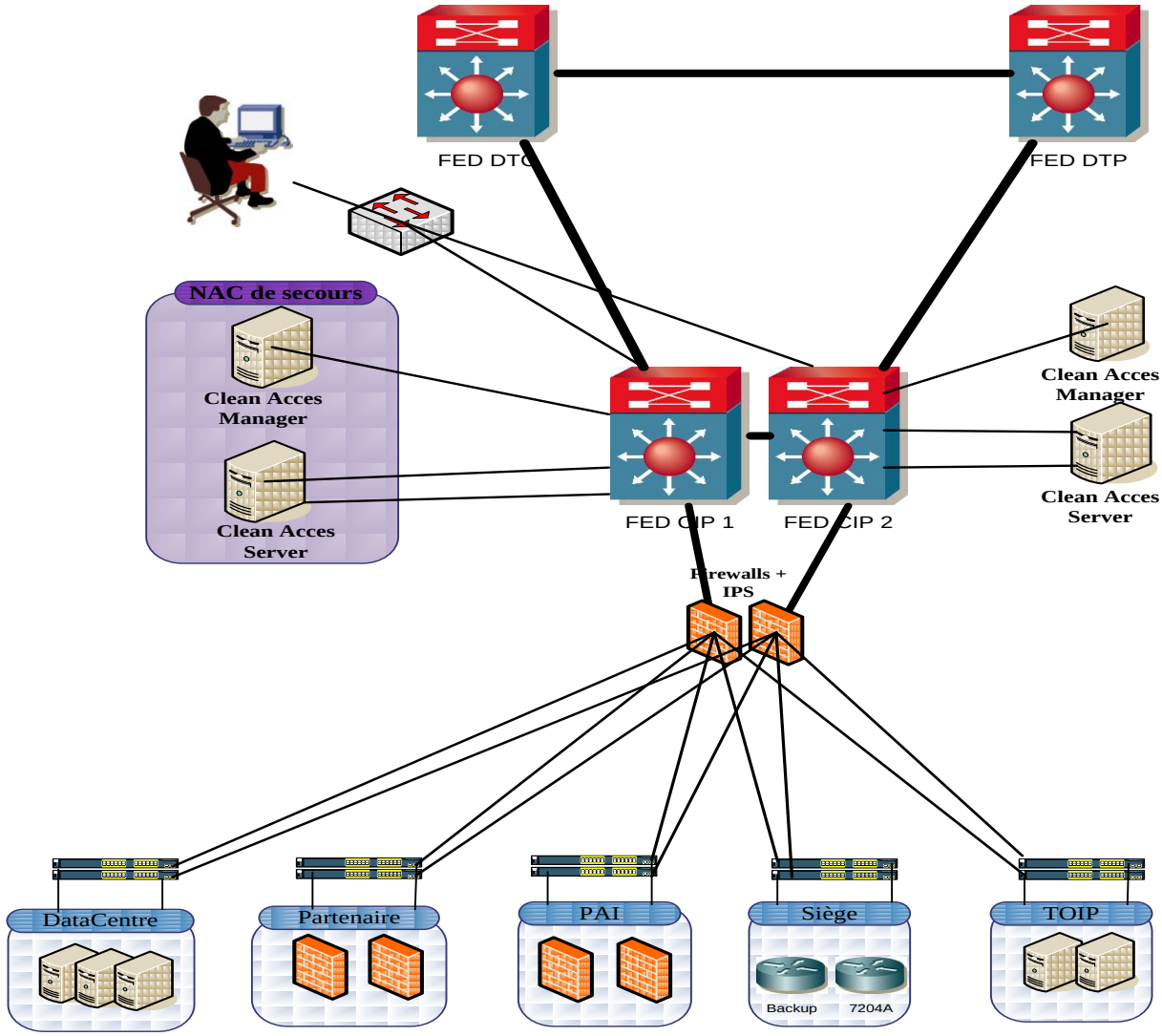


Figure 19 : Mise en place de technologie NAC

3. La sécurisation de la connexion aux partenaires

D'après la figure 4 présentée dans le chapitre 1 « Etude de l'existant », nous avons observé que La connexion de DEPC avec la société d'Echange de Données Informatisée (EDI) se fait par l'intermédiaire d'une liaison LS directement connecté en absence d'équipement permettant la sécurisation de cette connexion.

Les pirates utilisent sur internet du code malveillant (virus, vers et chevaux de Troie) pour forcer les portes des ordinateurs mal protégés.

Un Firewall vous aide à préserver votre ordinateur de ce type d'attaque et de bien d'autres.

Nous proposons alors de mettre le firewall SSG 140 existant ou un nouveau Firewall pour l'accès au partenaire (EDI) pour :

- **Contrôler les accès non autorisé qui peuvent divulguer des informations sensibles,**

- **Se protéger contre les virus et les intrusions indésirables,**

- **Minimiser le coût d'investissement.**

La figure ci-dessous présente le DMZ de partenaire :

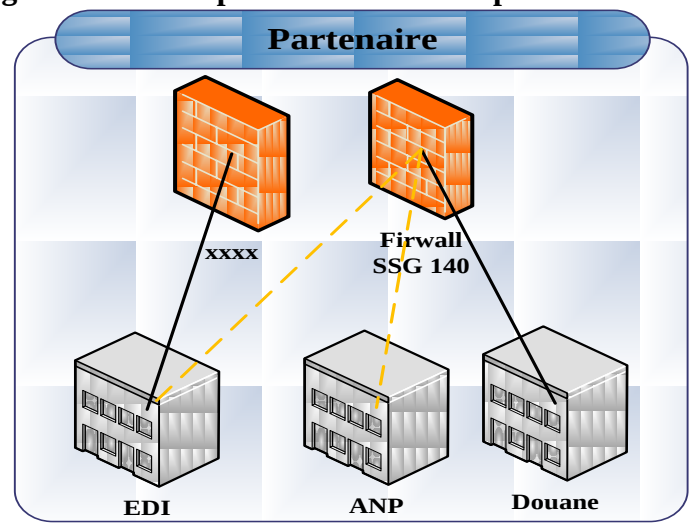


Figure 20 : Liaison Firewall à l'EDI

4. Gestion des Logs

4.1 Introduction

Un log est un Fichier créé par un logiciel spécifique comme NS LOG qui permet de garder une trace des événements s'étant produits sur un système, des requêtes qu'il reçoit et des opérations qu'il effectue.

Les logs contiennent des informations sur l'activité du serveur. Il ne fait aucun doute que l'analyse des logs de serveurs permet de générer de l'information fort utile aux gestionnaires et chercheurs. Par contre, certains développements technologiques récents et comportements des internautes doivent attirer l'attention des utilisateurs au sujet des rapports générés à partir des logs.

En effet, on doit savoir que plusieurs comportements ou technologies peuvent influencer grandement ce qui est inscrit dans le log du serveur ou encore le résultat obtenu suite à l'analyse des logs.

4.2 NSLOG

Editeur et constructeur de solutions de corrélation de logs, NSLOG est spécialisé dans l'analyse et le contrôle des logs des équipements de sécurité, de réseau et de serveurs.

La solution de NSLOG se décline en solutions logicielles et matérielles parfaitement intégrées et inter-opérables. Elle répond aux problématiques de clients Grands Comptes dans tous les secteurs d'activité.

NSLOG dispose d'une expertise particulièrement développée dans la conception de solutions de contrôle et de corrélation des logs des équipements de sécurité, de réseau et de serveurs (Security Information & Event Management).

Grâce à une technologie très modulaire, NS LOG construit des solutions adaptées à l'environnement et aux besoins de ses clients. Elles permettent d'administrer et de superviser la sécurité des applications de façon pertinente, en intégrant une approche nouvelle dans le domaine de la corrélation des événements de sécurité. NS LOG propose ainsi une approche de la sécurité des applications informatiques résolument efficace et unique pour répondre aux besoins exprimés par les clients.

5. L'amélioration de protocole de gestion SNMP

Le protocole SNMP (Simple Network Management Protocol) est très utilisé dans le milieu de l'administration réseau.

En effet, il permet de simplifier grandement la maintenance des réseaux en fournissant aux administrateurs la possibilité d'obtenir de nombreuses informations sur des équipements présents sur le réseau tels que des serveurs, des routeurs ou encore des commutateurs.

5.1 Les Faiblesses de SNMPv2

Au réseau de DEPC de Marsa Maroc, les transactions et le trafic qui circulent entre le client/ serveur utilisant le protocole SNMP version 2 risquent d'être sous une action malveillante, à cause d'absence d'un mécanisme adéquat pour assurer la confidentialité et la sécurité des fonctions de gestion. Les faiblesses comprennent aussi l'authentification et le cryptage, en plus de l'absence d'un cadre administratif pour l'autorisation et le contrôle d'accès.

5.2 Les améliorations de SNMPv3

Cette nouvelle version du protocole SNMP vise essentiellement à inclure la sécurité des transactions. La sécurité comprend l'identification des parties qui communiquent et l'assurance que la conversation soit privée, même si elle passe par un réseau public.

Cette sécurité est basée sur 2 concepts :

- USM (User-based Security Model),
- VACM (View- based Access Control Model).

5.2.1 User Security Module (USM)

Trois mécanismes sont utilisés. Chacun de ces mécanismes a pour but d'empêcher un type d'attaque.

- **L'authentification : Empêche quelqu'un de changer le paquet SNMPv3 en cours de route et de valider le mot de passe de la personne qui transmet la requête.**
- **Le cryptage : Empêche quiconque de lire les informations de gestions contenues dans un paquet SNMPv3 (utilisant le cryptage DES).**
- **L'estampillage du temps : Empêche la réutilisation d'un paquet SNMPv3 valide a déjà transmis par quelqu'un.**

5.2.2 VACM (View Access Control Model)

Permet le contrôle d'accès au MIB. Ainsi on a la possibilité de restreindre l'accès en lecture et/ou écriture pour un groupe ou par utilisateur.

6. Protéger le réseau : control d'accès

Pour visualiser les utilisateurs accédant au serveur et les ports utilisés, dont le but de limiter cet accès seulement pour les utilisateurs concerner, donc on configure un pare-feu central, dont on l'attribue des règles propres pour déterminer les paquets autorisés et les paquets interdits en utilisant des ACL (Access Control List); qui permettent de déterminer une liste d'accès des utilisateurs au ressources de réseau.

6.1 Protection de réseau

Les réseaux d'entreprises nécessitent l'attribut de droits pour certains membres de plusieurs groupes distincts, ce qui nécessite diverses astuces lourdes à mettre en œuvre des ACL.

Pour attribuer les ACL aux Firewalls principale, on a d'abord scanner le réseau à l'aide des outils de sécurité informatique qui sont, le 5VIEW et le packetshaper, dont le but est de savoir les utilisateurs auxquelles on attribue le droit de permission ou de refus, ainsi de fermer les ports ouverts.

6.1.1 Présentation des scanners

Le scanner est un dispositif permettant d'écouter le trafic d'un réseau en faisant des captures de trames qui y circulent. Il a pour fonctionnalité importante de réaliser un audit sur une station de travail ou sur un réseau tout entier en lançant des requêtes permettant de déterminer les services et les ports ouvert.

Le scan peut être utilisé sur une plage d'adresse IP nous permettant d'avoir une matrice de trafic de données à fin d'afficher les différents stations utilisant la bande passante et les applications exécutées sur ces dernières.

Pour des raisons de performance et de coût, nous avons choisi d'utiliser les logiciels 5View et Packetshaper pour auditer le réseau MARSA Maroc et déterminer le trafic qui y circule.

6.1.2 Présentation de l'outil 5view

5view est un outil d'exploration du réseau et permet de scanner les différents ports et applications ouvertes. Il est conçu pour permettre aux administrateurs système d'avoir une vue précise sur les applications, les protocoles et les services utilisés ainsi que le nom des stations connectées.

a. Description

5 view netflow présente en temps réel le trafic passant entre les utilisateurs et aussi entre les utilisateurs et les serveurs.

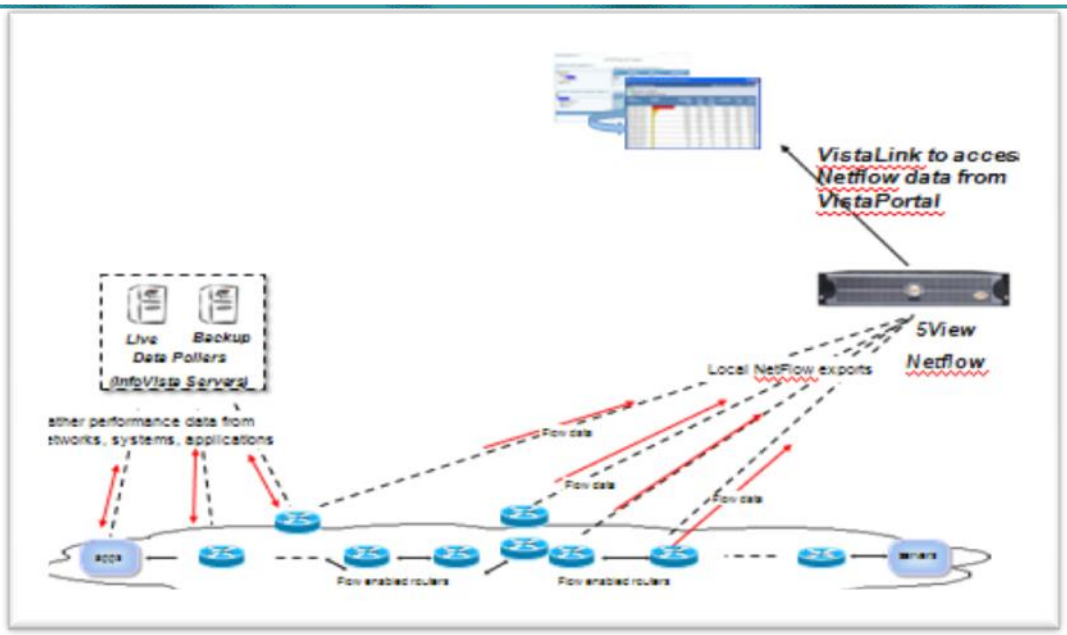


Figure 21 : Schéma présente la liaison entre le 5view et le réseau

b. La Qualités du scanner 5view

Le scanner 5VIEW détecte un maximum de flux entre client /serveur et client/client.

Le 5view a les qualités suivantes :

- **Gestion des mises à jour**

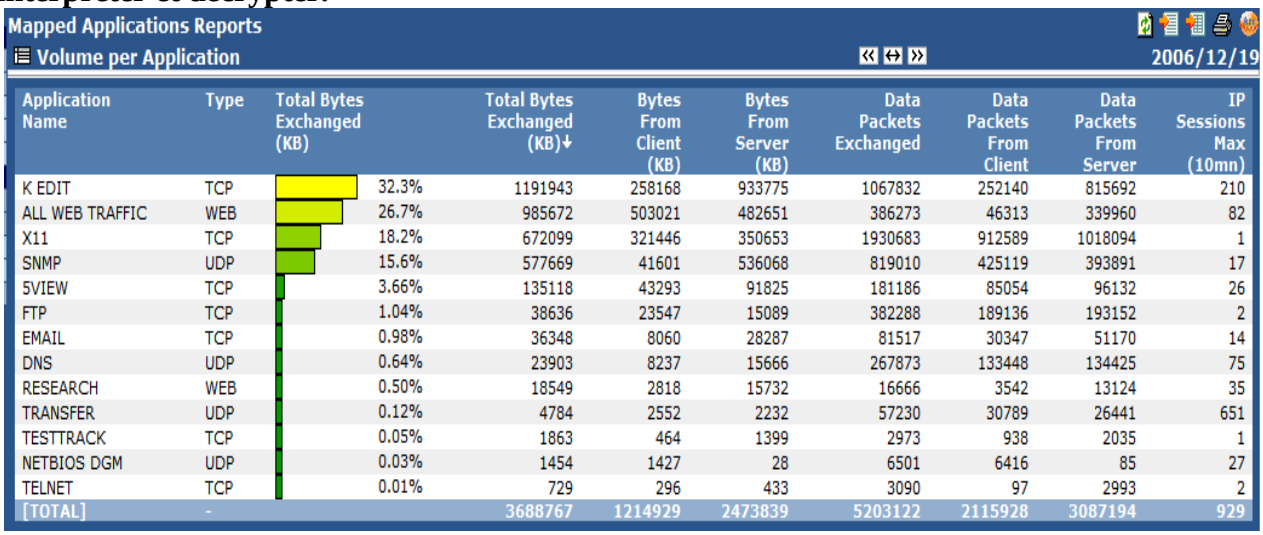
Comme les systèmes d'exploitation, le scanner 5VIEW repose sur une base de détection qui doit être mise à jour pour détecter et faire face à des nouvelles failles de sécurité.

Time Stamp	TCP/UDP Source Port	TCP/UDP Dest Port
18:01:24.203	27793	4589
18:01:24.531	27793	4589
18:01:26.421	2487	445
18:01:26.421	2487	445
18:01:26.421	2487	445
18:01:26.421	2487	445
18:01:28.718	4165	139
18:01:28.890	4165	139
18:01:29.703	12990	28232
18:01:32.265	27793	4589
18:01:32.546	27793	4589
18:01:34.390	8989	1927
18:01:35.218	2582	2368
18:01:39.718	52697	28232
18:01:43.562	27793	4589
18:01:45.906	2484	135
18:01:45.921	2491	445
18:01:45.921	2492	139
18:01:45.921	-	-
18:01:45.921	2493	139
18:01:45.921	2494	139
18:01:45.921	2492	139

Figure 22 : Schéma présente l'analyse en temps réel

- **Gestion et capacité de rapport**

5VIEW génère un rapport contenant toutes informations d'analyse du trafic qu'on peut interpréter et décrypter.



Mapped Applications Reports

Volume per Application — 2006/12/19

Application Name	Type	Total Bytes Exchanged (KB)		Total Bytes Exchanged (KB)↓	Bytes From Client (KB)	Bytes From Server (KB)	Data Packets Exchanged	Data Packets From Client	Data Packets From Server	IP Sessions Max (10mn)
K EDIT	TCP		32.3%	1191943	258168	933775	1067832	252140	815692	210
ALL WEB TRAFFIC	WEB		26.7%	985672	503021	482651	386273	46313	339960	82
X11	TCP		18.2%	672099	321446	350653	1930683	912589	1018094	1
SNMP	UDP		15.6%	577669	41601	536068	819010	425119	393891	17
5VIEW	TCP		3.66%	135118	43293	91825	181186	85054	96132	26
FTP	TCP		1.04%	38636	23547	15089	382288	189136	193152	2
EMAIL	TCP		0.98%	36348	8060	28287	81517	30347	51170	14
DNS	UDP		0.64%	23903	8237	15666	267873	133448	134425	75
RESEARCH	WEB		0.50%	18549	2818	15732	16666	3542	13124	35
TRANSFER	UDP		0.12%	4784	2552	2232	57230	30789	26441	651
TESTTRACK	TCP		0.05%	1863	464	1399	2973	938	2035	1
NETBIOS DGM	UDP		0.03%	1454	1427	28	6501	6416	85	27
TELNET	TCP		0.01%	729	296	433	3090	97	2993	2
[TOTAL]	-			3688767	1214929	2473839	5203122	2115928	3087194	929

Figure 23 : Schéma présente le rapport d'analyse

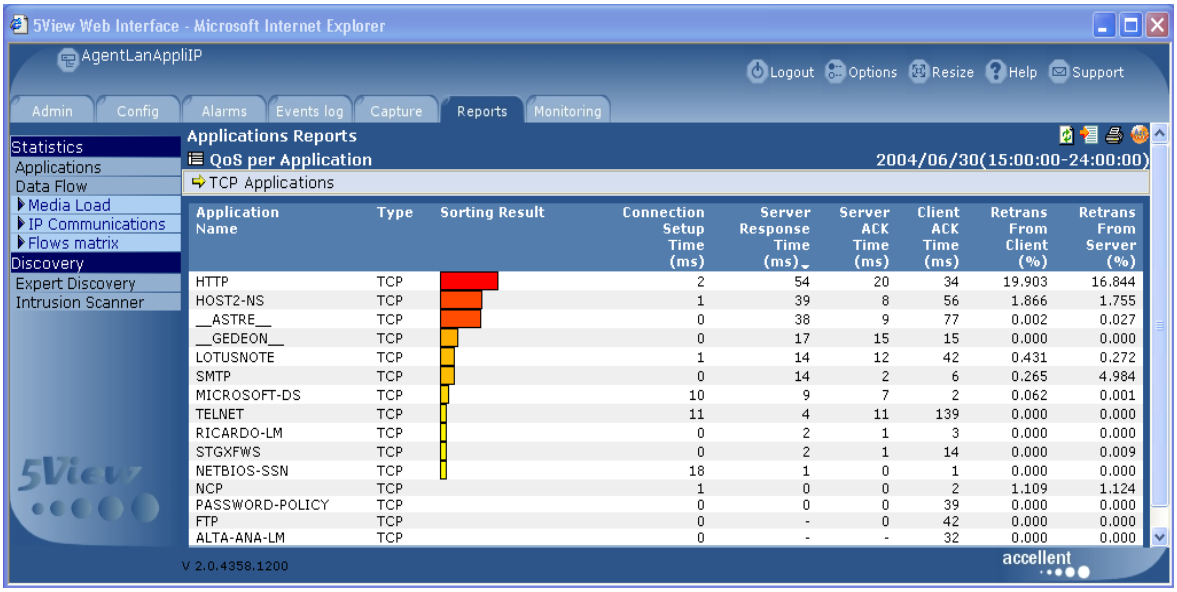
c. Applications

Le 5View permet de :

- Détecter les flux entrant et sortant des serveurs en fonction et hors fonction.
- Détecter les adresses IP inconnu (IP non interpréter par le DNS « Domaine Name Système).
- Définir une liste des applications à surveiller,
- Afficher la « QOS », le volume et le débit des statistiques sur les demandes définies.
- Afficher la matrice de flux entre les services, région ou pays.

d. Teste effectué et résultats observés

Pour mettre en pratique le serveur 5View, nous avons lancé un audit sur le réseau local de MARSA Maroc. En effectuant des captures de trames, nous avons pu extraire le trafic et les matrices de flux sur les différentes stations connectés sur le réseau.



5View Web Interface - Microsoft Internet Explorer

AgentLanAppliP — Logout Options Resize Help Support

Admin | Config | Alarms | Events log | Capture | Reports | Monitoring

Statistics: Applications, Data Flow, Media Load, IP Communications, Flows matrix

Discovery: Expert Discovery, Intrusion Scanner

Applications Reports

QoS per Application — 2004/06/30(15:00:00-24:00:00)

TCP Applications

Application Name	Type	Sorting Result	Connection Setup Time (ms)	Server Response Time (ms)↓	Server ACK Time (ms)	Client ACK Time (ms)	Retrans From Client (%)	Retrans From Server (%)
HTTP	TCP		2	54	20	34	19.903	16.844
HOST2-NS	TCP		1	39	8	56	1.866	1.755
__ASTRE__	TCP		0	38	9	77	0.002	0.027
__GEDEON__	TCP		0	17	15	15	0.000	0.000
LOTUSNOTE	TCP		1	14	12	42	0.431	0.272
SMTP	TCP		0	14	2	6	0.265	4.984
MICROSOFT-DS	TCP		10	9	7	2	0.062	0.001
TELNET	TCP		11	4	11	139	0.000	0.000
RICARDO-LM	TCP		0	2	1	3	0.000	0.000
STGXFWS	TCP		0	2	1	14	0.000	0.009
NETBIOS-SSN	TCP		18	1	0	1	0.000	0.000
NCP	TCP		1	0	0	2	1.109	1.124
PASSWORD-POLICY	TCP		0	0	0	39	0.000	0.000
FTP	TCP		0	-	0	42	0.000	0.000
ALTA-ANA-LM	TCP		0	-	-	32	0.000	0.000

5View — V 2.0.4358.1200 — accellent

Figure 24 : Schéma présente le trafic visualisé après la capture

Après une capture en utilisant 5View sur un serveur choisi « BOSERVER » de MARSA Maroc, nous avons obtenu le tableau ci-dessous qui présente tout les clients utilisant des applications à travers les quelles se connectent aux serveurs.

Cette capture présente également les différents ports et protocoles de communication utilisés.

Serveur	Application	Clients	Protocoles	Ports
Boserver	repsvc	172.016.002.034	TCP	6320
	NetBios -	172.016.132.036		
		172.016.002.032		
		172.016.132.180		
		172.016.002.017		
		172.016.192.199		
		172.017.017.053		
		172.020.104.106		
		172.016.162.070		
		172.016.192.074		
		172.020.104.105		
		172.016.162.125		
		172.016.002.247		
		172.016.193.021		
		172.016.005.021		
		172.017.051.056		
		172.016.005.009		
		172.016.000.254		
	HTTP	172.016.005.009	tCP	80
		172.016.162.070		
		172.016.192.074		
	pim-port	172.016.001.252	tCP	8471
	ICMP	172.016.002.034	ip:1	8471
		172.017.253.252		
		172.016.001.199		
		172.017.017.053		
		172.020.104.106		
		172.019.020.024		
		172.020.104.105		
		172.016.132.036		
		172.017.253.250		
		172.019.040.053		
		172.019.040.011		
		172.016.002.032		
		172.016.192.199		
		172.016.132.180		
		172.016.162.070		
		172.016.192.074		

		172.016.005.009		
		172.016.162.125		
		172.016.002.017		
		172.016.133.038		
		172.016.193.174		
		172.016.192.072		
		172.016.193.189		
		172.016.162.199		
		172.016.132.036		
		172.016.132.179		
		172.016.132.078		
		172.016.132.211		
		172.016.133.065		
		172.016.132.074		
		172.016.133.077		
		172.016.132.064		
	Microsoft SQL Server	172.016.001.241	TCP	
	repsvc			
	Windows Services			
	LDAP			
	Kerberos			
	DNS			
	vdmplay			
	netattachsdmp			

Tableau 6 : Résultat d'analyse de trafic pour le serveur Boserver

6.1.3 Présentation de l'outil Packetshaper

a. Description général

Le Packetshaper est un dispositif de gestion du trafic qui permet de résoudre les problèmes avec tout le contrôle possible. En effet, ce dispositif contrôle et comprime le trafic réseau, en offrant un service de haute qualité pour les applications et permet aux entreprises de mettre en ligne les ressources de leur réseau et les besoins de leurs activités.

Le Packetshaper organise automatiquement le trafic réseau en catégories basées sur l'application, le protocole, le sous-réseau, l'URL et d'autres critères, créant ainsi des milliers de catégories potentielles.

Du point de vue économique, le packetshaper a beaucoup d'avantages on peut citer comme exemples:

L'augmentation du réseau existant et des ressources en bande passante.

- Il évite les augmentations de bande passante et les mises à jour de l'infrastructure.
- Il sauvegarde la bande passante et d'autres éléments du réseau qui prennent en charge les applications d'entreprises et non pas le trafic anarchique.

L'approche en quatre étapes de Packetshaper afin de protéger les performances des applications

- **PREMIERE ETAPE : CLASSIFICATION**

Packetshaper classifie automatiquement le trafic réseau en catégories basées sur l'application, le protocole, le sous-réseau, l'URL et d'autres critères, créant ainsi des milliers de catégories potentielles. Packetshaper va au-delà de la correspondance de ports et des adresses IP.

- **DEUXIEME ETAPE : ANALYSE**

Packetshaper recueille plus de 60 métriques pour chaque type de trafic afin de fournir une analyse détaillée de l'utilisation du réseau, des performances des applications et de l'efficacité du réseau.

- **TROISIEME ETAPE : RAPPORT**

Packetshaper peut générer des rapports internes volumineux : rapports, graphiques et statistiques via SNMP et XML.

b. Le test effectué

Avec le dispositif Packetshaper, nous avons pu avoir une analyse sur le trafic qui circule dans le réseau et affiche les différents services utilisés, qui sont déterminés comme des sous-classes au classe père (Inbound et Outbound). En spécifiant l'adresse de l'hôte afin d'obtenir son trafic, on obtiendra le résultat suivant:

Figure 25: Résultat d'analyse de trafic réseau à l'aide de Packetshaper

6.1.4 Observations

D'après le résultat obtenu à l'aide des deux outils de scan (5View et Packetshaper), nous avons constaté que le 5View est plus performant que le Packetshaper, car ce dernier bloque et plante le réseau en cour de capture de trafic. De ce fait Packetshaper ne peut pas traiter toutes les applications.

Etant donné cela, nous avons choisis le 5View pour analyser le réseau DEPC de MARSA Maroc, à fin de pouvoir déterminer une stratégie des droits d'accès (ACL) au niveau des Firewall Principaux.

N.B : Pour fermer les ports ouverts non fonctionnel nous avons utilisé le scan NMAP (voir détail annexe B).

6.1.5 Les droits d'accès

La protection consiste à empêcher qu'un utilisateur puisse altérer un fichier qui ne lui appartient pas sans que le propriétaire lui en ait donné l'autorisation, ou encore, par exemple, à empêcher qu'un processus en cours d'exécution ne modifie une zone mémoire attribuée à un autre processus sans l'autorisation du propriétaire de celui-ci.

Le propriétaire d'un objet peut avoir conféré à lui-même et à d'autres utilisateurs des droits d'accès à cet objet. Les types de droits possibles sont en général les suivants (on peut en imaginer d'autres) :

- **droit d'accès en consultation (lecture) ;**
- **droit d'accès en modification (écriture, destruction, création) ;**

- **droit d'accès en exécution ; pour un programme exécutable, la signification de ce droit est évidente pour un répertoire de fichiers ce droit confère à ceux qui le possèdent la faculté d'exécuter une commande ou un programme qui consulte ce répertoire ;**

- **droit de blocage, par exemple pour un processus en cours d'exécution ou éligible pour l'exécution.**

À chaque firewall est donc associée une liste de contrôle d'accès (Access control List « ACL ») qui énumère les utilisateurs autorisés et leurs droits pour éviter la charge de la bande passante, aussi il y a le problème de connexion à distance avec telnet qui permet à un internaute de se connecter, et donc d'utiliser à distance une machine comme s'il se trouvait face à elle.

7. La connexion à distance

La connexion à distance à MARSA MAROC se fait à l'aide du protocole TELNET, mais ce dernier a plusieurs inconvénients parmi elle; la mauvaise sécurité, en fait avec TELNET toutes les informations transmises transitent en clair sur le réseau, y compris les mots de passe, ce qui permet à un éventuel pirate simplement à l'écoute du réseau d'intercepter toutes les données sensibles qui transiteraient de cette manière.

C'est pour cette raison on a pensé à utiliser le protocole SSH dont toutes les données transmises sont cryptées et donc illisibles par toute autre personne que le destinataire.

Les deux services permettent à un internaute (utilisateur d'Internet) de se connecter et donc d'utiliser à distance une machine comme s'il se trouvait face à elle. Cela ouvre par exemple des possibilités pour le travail à domicile, puisqu'il devient possible d'utiliser les machines se trouvant sur son lieu de travail depuis chez soi.

8. La solution Firewall /IPS

Les techniques traditionnelles de filtrage n'étaient plus suffisamment efficaces pour bloquer les attaques moderne perfectionnées, et que les pare-feu modernes utilisaient de plus en plus les techniques qui permettent d'arrêter les intrusions entre les différentes VLAN, d'où on a pensé à utiliser un firewall qui intègre les fonctionnalités des IPS (Intrusion Prévention System) qui est une solution de prévention des intrusions.

IPS est un mécanisme écoutant le trafic réseau de manière furtive afin de repérer des activités anormales ou suspectes et permettant ainsi d'avoir une action de prévention sur les risques d'intrusion.

Cet outil ce caractérise par la possibilité de bloquer immédiatement les intrusions et ce quel que soit le type de protocole de transport utilisé, ce qui induit que l'IPS est constitué en natif d'une technique de filtrage de paquets et de moyens de blocages.

9. La mise en place de la solution Datacenter avec la technologie Nexus

9.1 Introduction

Un data center (en français: "centre de données" ou "centre de traitement de données") c'est tout d'abord un centre qui centralise des données informatique. C'est généralement l'endroit où sont placés les serveurs.

Les premiers data center avaient pour objectif d'offrir un centre d'hébergement et de traitement des données hyper sensibles à de grandes entreprises internationales, d'un niveau de sécurité très élevé.

Au fil du temps et de la démocratisation des composantes ainsi que la virtualisation des serveurs, les Datacenter se sont positionnés comme étant une solution économique pour les PME et petits indépendants. Il est aujourd'hui plus intéressant d'utiliser les services ainsi que la qualité d'un data center plutôt que d'investir dans du matériel propre.

Ces centres de données regroupent une multitude de machines. Les données mises en place sur les serveurs doivent être accessible à tout moment et protégées des dégâts extérieurs, par conséquent les data center ont pour principalement force d'être prévu de façon à être protégée des principaux risques de coupure ou d'intrusion. Il y a ainsi des protections contre les coupures électriques, les risques d'incendie, l'accès de personnes malveillantes sur les serveurs.

Figure 26 : Intérieur d'un data center

Les serveurs sont généralement rangées dans des baies (ressemble à une grosse armoire) et les connexions sont prévus pour faciliter la rapidité d'accès aux machines.

9.2 L'avantage d'un Datacenter

L'avantage principal d'un data center est bien évidemment la qualité des infrastructures et le niveau de sécurité. Cela devient encore plus avantageux pour une PME car il lui serait impossible de se doter d'un local informatique équivalent.

Sans parler des ressources nécessaires afin d'administrer et de sécuriser le matériel et l'infrastructure.

- Serveur performant
- Connexion internet haut débit
- Investissement nul
- Pas de frais d'installation
- Pas de frais de maintenance
- Utilisation sur mesure

- Gain de place
- Sécurité maximale

9.3 Technologie Nexus

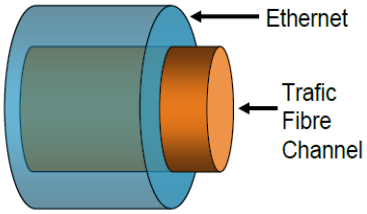
Les annonces récentes faites par plusieurs constructeurs dont Cisco avec la famille de produit Nexus ouvrent de nouvelles perspectives sur l'architecture réseau des centres informatiques : accompagner les phénomènes de consolidation et de virtualisation, augmenter la résilience des flux et simplifier les architectures réseaux LAN et SAN.

Tout d'abord, le Nexus 7000 (annoncé en Janvier 2008) adresse les challenges de la haute densité, de la haute performance et de la disponibilité au cœur du réseau LAN du Datacenter.

Lancée encore plus récemment (avril 2008), la série Nexus 5000 permet la mutualisation des flux SAN et LAN sur les mêmes liens physiques Ethernet : cette gamme met en avant de nouvelles technologies accompagnées de ces nouveaux vocables dont les principaux sont FCoE et Cisco Data Center Ethernet.

FCoE (Fibre Channel over Ethernet), a pour but le transport de Fibre Chanel Protocol directement sur un réseau Ethernet dit 'lossless' ou « sans perte de paquet », ce qui signifie que l'acheminement des trames doit être garanti. Pour rappel, le Fibre Channel Protocol (FCP) est le protocole assurant aujourd'hui le transport des données au sein des réseaux de stockage (SAN).

Fibre Channel over Ethernet :



- **Méthode pour transport les trames FC sur Ethernet**
- **Les trames FC sont inchangées**
- **Pas de translation de Protocole**
- **FCoE apparaît comme du FC pour les Serveurs et les Baies de Stockage**
- **Préserve l'Infrastructure existante et les Systèmes d'Administration**

Le Nexus 5000 permet la consolidation de l'Ethernet et de la Fibre Channel, à être transportée à travers la même pièce physique du câble Ethernet.

9.4 L'architecture proposée: Top-Of-the-Rack (TOR)

Afin d'accroitre la flexibilité, la conception du Centre Informatique de façon plus modulaire s'impose afin de répondre plus rapidement aux changements technologiques et pérenniser les infrastructures du Centre Informatique en terme d'alimentation, de refroidissement et de câblage.

De nombreuses organisations aujourd'hui ne déploient plus de serveurs de manière unitaire mais des racks complets de serveurs ou des systèmes « blades » préconfigurés qui intègrent l'ensemble de la connectivité et permet d'améliorer la mise en production des nouvelles ressources à l'intérieur du Centre Informatique.

La granularité devenant le rack, il devient nécessaire de repenser les modèles de câblage afin de s'adapter à l'augmentation de la densité et maximiser l'utilisation des ressources disponibles dans le Centre Informatique.

Le modèle ToR facilite l'adoption de ce mode dont le déploiement est connu sous le nom de Rack-and-Roll et minimise le nombre de câble entre l'EDA et la HDA. Les ressources assurant la connectivité serveurs aux différents réseaux sont placées dans le rack et interconnectées à ces réseaux par quelques fibres. Si ce modèle tend à se généraliser pour le LAN, il reste néanmoins plus rare pour le SAN, car tous les serveurs ne sont pas forcément candidats à l'accès aux ressources de stockage en mode Fibre Channel, notamment à cause du coût des HBA Fibre Channel.

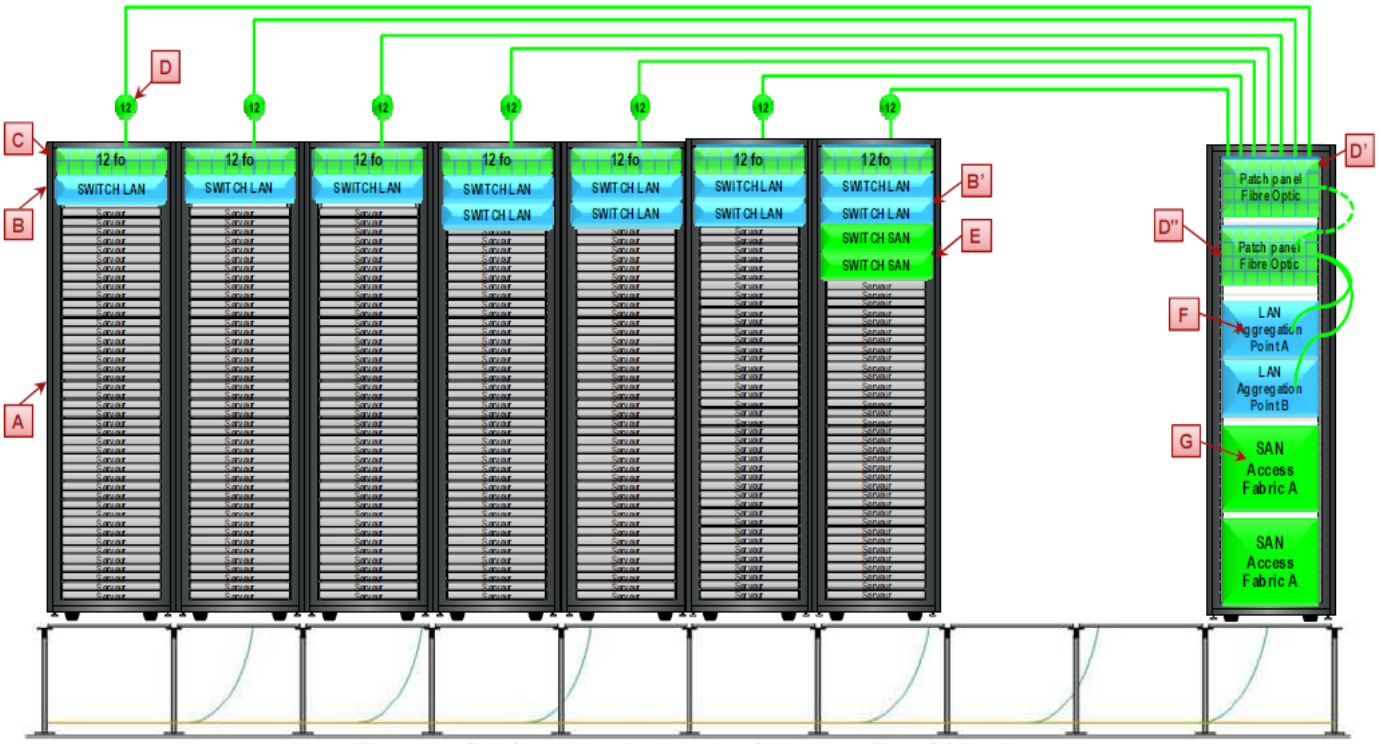


Figure 27 : Schéma de principe du câblage en Top Of Rack

Rack serveur contenant jusqu'à 40 serveurs. Chacun de ces serveurs possèdent entre 2 & 3 connexion LAN, et certains sont connectés à deux Fabrics SAN. La taille des racks recommandés est de 80 cm. Le nombre de racks dans une rangée dépend de chaque Centre Informatique, en général entre 10 et 30 (12 en moyenne).

B — Commutateur LAN placé en Top of Rack, de 24 ports à 48 ports (Catalyst 3750E, Catalyst 4948, Nexus 2k, Nexus 5K ;…).

B' — Dans le cas d'un réseau haute disponibilité le commutateur d'accès est doublé.

C — Patch-Panels de connexion Fibre Optique, typiquement 12 ports LC permettant le raccordement aux SAN (2 fabrics) de 6 serveurs. En fonction de la densité des serveurs et du taux de raccordement au SAN, le nombre de connexion Fibre Optique peut augmenter.

D — Câble Fibre Optique permettant de raccorder du patch panel D au patch panel D'. L'utilisation de connecteurs MTP et d'épanouisseurs optiques permet d'envisager une transition vers le 40Gbits sans remise en cause du précâblage.

D' — Patch-Panels de connexion FO assurant le raccordement en fin de rangée des patch-panels situés dans les racks (A).

D" Patch-Panels de connexion FO assurant une connexion fixe avec les équipements SAN(F) et SAN (G)

E Commutateur SAN placé en Top of Rack, en général de 24 ports à 48 ports.

F Equipements LAN dimensionnés en fonction du nombre de racks dans la rangée. Ils seront constitués de commutateurs modulaires (Catalyst 4500 ou 6500, Nexus 7K),

G Equipements SAN dimensionnés en fonction du nombre de racks et ports dans la rangée. Ils seront constitués de commutateurs modulaires.

Conclusion

Après avoir cerné les différents points critiques et les failles de sécurité du parc informatique de Marsa Maroc. Nous avons proposé des recommandations afin obtenir une architecture réseau sécurisé et optimale, en utilisant des équipements de redondances et des infrastructures de sécurité.

Cependant, pour mieux sécuriser le réseau métropolitain (MAN) de Marsa Maroc, nous avons proposé également la mise en place d'une nouvelle technologie de contrôle d'admission NAC (Network Admission Control) qui vérifie avant d'accéder au réseau que la machine est saine.

En ce qui concerne, la gestion des droits et des autorisations aux utilisateurs de Marsa Maroc, nous avons proposé la mise en place d'un Contrôleur de Domaine (DC) en installant un serveur Windows 2008 et d'y installer le service d'annuaire "Active Directory" qui nous permet de centraliser et gérer les utilisateurs et les ressources informatiques de l'entreprise.

Pour limiter l'accès des utilisateurs aux différents services, nous avons déployé des outils de scan à savoir 5view et Packetshaper, afin de relever des informations utiles pour restreindre le trafic sortant/entrant au niveau des firewalls centraux.

Ce projet a été l'occasion de mettre en pratique la formation théorique que nous avons reçue à l'FST qui s'est révélée adaptée aux compétences souhaitées.

Références bibliographiques

Documentations :

Des informations sous format électroniques auprès de Marsa Maroc

Web :

http://www.frameip.com/firewall/
http://en.wikipedia.org/wiki/Network_Access_Control
http://www.cisco.com/en/US/products/ps9441/Products_Sub_Category_Home.html
http://fr.wikipedia.org/wiki/Simple_network_management_protocol
http://fr.wikipedia.org/wiki/IPS
http://fr.wikipedia.org/wiki/Administrateur_r%C3%A9seaux
Documentation de référence nmap : http://insecure.org/nmap/man/fr/man-port-scanning-techniques.html

Annexes

Annexe A:

Tableaux

Equipement	Type	Adresse IP	Emplacement
C2900-Garage	WS-C2924M-XL	172.16.1.195	Garage (station)
FED-4507R-CIP	WS-C4507R-E	172.16.128.1	Centre Informatique
Switch-Serveurs	WS-C3560G-24PS	172.16.128.8	Centre Informatique
SW-C3750-FACT	WS-C3750-48P	172.16.128.10	Facturation
SW-C3750-CIP1	WS-C3750-48P	172.16.128.11	Bâtiment pricipal
SW-C3750-JURID	WS-C3750-24P	172.16.128.12	Juridique
SW-C3750-DRH	WS-C3750-24P	172.16.128.13	DRH
FED-4507R-DTC	WS-C4507R-E	172.16.160.1	DTC
SW-C3750-SAGETEC	WS-C3750-48PS	172.16.160.10	SAGETEC
SW-3560-ZC1	WS-C3560-8PC	172.16.160.11	Zone de charge 1
SW-3560-ZC2	WS-C3560-8PC	172.16.160.12	Zone de charge 2
SW-3560-ZC3	WS-C3560-8PC	172.16.160.13	Zone de charge 3
SW-C3560-PB10	WS-C3560-8PC	172.16.160.14	Pont Bascule 10
SW-C3560-RORO	WS-C3560-8PC	172.16.160.17	Magasin RORO
SW-3560-TCE1	WS-C3750-48P	172.16.160.21	Guichet unique
SW-3560G-TCE2.	WS-C3560G-24PS	172.16.160.22	Guichet unique
SW-C3750-DMH	WS-C3750-24P	172.16.160.24	DMH
SW-C3750-TECH	WS-C3750-24P	172.16.160.27	Bâtiment Technique
SW-3560-Dexport-	WS-C3560-8PC	172.16.160.32	Dexport
SW-3560-Visite-	WS-C3560-8PC	172.16.160.33	Visite
SW-C3560-ACCESDTC	WS-C3560-8PC	172.16.160.40	Accès DTC
SW-3560-B/Charge	WS-C3560-8PC	172.16.160.41	Bon de charge
SW-RORO	WS-C3750-24P	172.16.160.50	DELDTC
FED-4507R-DTP	WS-C4507R-E	172.16.200.1	DTP/DO
SW-C3750-DTMD	WS-C3750-48P	172.16.200.10	DTMD
SW-C3750-DER	WS-C3750-24P	172.16.200.11	DER

SW-C3560-SER-ELEC	WS-C3560-8PC	172.16.200.12	Service Electrique
SW-C3560-MG14	WS-C3560-8PC	172.16.200.13	Magasin 14
SW-C3750-DER	WS-C3560-48PS	172.16.200.66	Nouveau DER
SW-CIM-200.20	WS-C3560-8PC	172.16.200.20	Magasin CIM (30)
SW-C3560-inflam	WS-C3560-8PC	172.16.200.21	Zone inflammable
SW-3560-MG10-	WS-C3560-8PC	172.16.200.23	Magasin 10
SW-3560-TP16-	WS-C3560-8PC	172.16.200.24	Terre pleine 16
SW-C3560-MG07	WS-C3560-8PC	172.16.200.60	Magasin 7
SW-3560-Mag05	WS-C3560-8PC	172.16.200.61	Magasin 5
SW-C3560-PB14	WS-C3560-8PC	172.16.200.62	Pont Bascule 14
SW-C3560-Infirmerie	WS-C3560-8PC	172.16.200.63	INFIRMERIE
SW-C3560-PB15	WS-C3560-8PC	172.16.200.64	Pont Bascule 5A(15)
SW-C3560-MAG-GEN-	WS-C3560-8PC	172.16.200.65	Magasin Général
SW-PB05-200.67	WS-C3560-8PC	172.16.200.67	Pont Bascule 05
SW-C3560-ACCESDTP	WS-C3560-8PC	172.16.200.30	Accès DTP
DEPC.yourdomain.com	Cisco 3850	172.16.1.206	Bâtiment pricipal
Marsamaroc	Cisco 2821	172.16.15.1	Central Téléphonique
TO-GNS	Cisco 1601	172.16.1.108	CIP
Juniper		172.16.1.41	CIP
Bridge CIP1		172.16.255.26	Centre Informatique
Bridge CIP2		172.16.255.34	Centre Informatique
Bridge DTP1		172.16.255.28	DTP/DO
Bridge DTP2		172.16.255.27	DTP/DO
Bridge DTC1		172.16.255.37	DTC
Bridge DTC2		172.16.255.25	DTC

Tableau 4 : Correspondance Switch Adresse IP

Equipement	Type	Equipements adjacent
TO-GNS	1601	FED-4507R-CIP.sodep.co.ma,
FED-4507R-CIP.sodep.co.ma	C4507R-E	SW-C3750-FACT-128.10.sodep.co.ma SW-C3750-CIP1-128.11.sodep.co.ma

		FED-4507R-DTP.sodep.co.ma FED-4507R-DTC.sodep.co.ma SW-C3750-JURID-128.12.sodep.co.ma TO-GNS, Switch-Serveurs
Unknown	Unknown	Unknown
marsamaroc.depc.ma	2821	SW-C3750-CIP1-128.11.sodep.co.ma
Switch-Serveurs	C3560G-24PS	FED-4507R-CIP.sodep.co.ma
SW-C3750-FACT-128.10.sodep.co.ma	C3750-STACK	FED-4507R-CIP.sodep.co.ma
SW-C3750-CIP1-128.11.sodep.co.ma	C3750-STACK	marsamaroc.depc.ma BridgeCIP2 FED-4507R-CIP.sodep.co.ma BridgeCIP1
SW-C3750-JURID-128.12.sodep.co.ma	C3750-STACK	SW-C3750-DRH-128.13.sodep.co.ma FED-4507R-CIP.sodep.co.ma
SW-C3750-DRH-128.13.sodep.co.ma	C3750-STACK	SW-C3750-JURID-128.12.sodep.co.ma
Unknown	Unknown	Unknown
Unknown	C2950G-48	Unknown
Unknown	Unknown	Unknown
FED-4507R-DTC.sodep.co.ma	C4507R-E	SW-C3750-DMH-160.24.sodep.co.ma SW-C3560-ZVIDE-160.31 SW-3560-Dexport-160.32.sodep.co.ma SW-C3750-TECH-160.27.sodep.co.ma SW-3560-Visite-160.33.sodep.co.ma SW-C3750-SAGETES-160.10.sodep.co.ma SW-RORO-160.50 SW-3560-ZC2-160.12 SW-3560-B/Charge.sodep.co.ma SW-3560-ZC1-160.11.sodep.co.ma FED-4507R-DTP.sodep.co.ma SFED-4507R-CIP.sodep.co.ma
SW-C3750-SAGETES-160.10.sodep.co.ma	C3750-STACK	FED-4507R-DTC.sodep.co.ma
SW-3560-ZC1-160.11.sodep.co.ma	C3560-8PC	FED-4507R-DTC.sodep.co.ma
SW-3560-ZC2-160.12	C3560-8PC	FED-4507R-DTC.sodep.co.ma
SW-3560-ZC3-160.13.sodep.co.ma	C3560-8PC	FED-4507R-DTC.sodep.co.ma
Unknown	Unknown	Unknown
SW-3560-TCE1-160.21	C3750-STACK	SW-3560G-TCE2.160.22 FED-4507R-DTC.sodep.co.ma
SW-3560G-TCE2.160.22	C3560G-24PS	SW-3560-TCE1-160.21
SW-C3750-DMH-160.24.sodep.co.ma	C3750-STACK	FED-4507R-DTC.sodep.co.ma
Unknown	Unknown	Unknown
SW-C3750-TECH-160.27.sodep.co.ma	C3750-STACK	FED-4507R-DTC.sodep.co.ma
SW-C3560-ZVIDE-160.31	C3560-8PC	FED-4507R-DTC.sodep.co.ma
SW-3560-Dexport-160.32.sodep.co.ma	C3560-8PC	FED-4507R-DTC.sodep.co.ma
SW-3560-Visite-160.33.sodep.co.ma	C3560-8PC	FED-4507R-DTC.sodep.co.ma
Unknown	Unknown	Unknown

SW-C3560-ACCESDTC-160.40.sodep.co.ma	Unknown	Unknown
SW-3560-B/Charge.sodep.co.ma	C3560-8PC	FED-4507R-DTC.sodep.co.ma
SW-RORO-160.50	C3750-STACK	FED-4507R-DTC.sodep.co.ma
Unknown	Unknown	Unknown
FED-4507R-DTP.sodep.co.ma	C4507R-E	SW-C3750-DTMD-200.10.sodep.co.ma SW-3560-Mag05-200.61.sodep.co.ma SW-C3750-DER-200.11.sodep.co.ma SW-3560-TP16-200.24.sodep.co.ma SW-CIM-200.20 FED-4507R-CIP.sodep.co.ma FED-4507R-DTC.sodep.co.ma SW-C3560-MG07-200.60.sodep.co.ma SW-3560-SER-ELEC-200.12.sodep.co.ma SW-PB14-200.62 SW-3560-MG10-200.23.sodep.co.ma BridgeDTP1 SW-PB15-200.64.sodep.co.ma SW-3560-INFIRMERIE-200.63.sodep.co.ma SW-C3750-DER-200.66 SW-3560-Mag-Gen-200.65.sodep.co.ma SW-3560-Bung-DTMD-200.30.sodep.co.ma
SW-C3750-DTMD-200.10.sodep.co.ma	C3750-STACK	FED-4507R-DTP.sodep.co.ma
SW-C3750-DER-200.11.sodep.co.ma	C3750-STACK	FED-4507R-DTP.sodep.co.ma
SW-3560-SER-ELEC-200.12.sodep.co.ma	C3560-8PC	FED-4507R-DTP.sodep.co.ma
Unknown	Unknown	Unknown
Unknown	Unknown	Unknown
SW-CIM-200.20	C3560-8PC	FED-4507R-DTP.sodep.co.ma
Unknown	Unknown	FED-4507R-DTP.sodep.co.ma
Unknown	Unknown	FED-4507R-DTP.sodep.co.ma
SW-3560-MG10-200.23.sodep.co.ma	C3560-8PC	FED-4507R-DTP.sodep.co.ma
SW-3560-TP16-200.24.sodep.co.ma	C3560-8PC	FED-4507R-DTP.sodep.co.ma
SW-3560-Bung-DTMD-200.30.sodep.co.ma	C3560-8PC	FED-4507R-DTP.sodep.co.ma
SW-C3560-MG07-200.60.sodep.co.ma	C3560-8PC	FED-4507R-DTP.sodep.co.ma
SW-3560-Mag05-200.61.sodep.co.ma	C3560-8PC	FED-4507R-DTP.sodep.co.ma
SW-PB15-200.64.sodep.co.ma	C3560-8PC	Unknown
SW-3560-Mag-Gen-200.65.sodep.co.ma	C3560-8PC	Unknown
SW-C3750-DER-200.66	C3560-48PS	Unknown
BridgeCIP1	Unknown	Unknown
BridgeDTP1	Unknown	Unknown
Unknown	Unknown	Unknown
BridgeCIP2	Unknown	Unknown
BridgeDTC2	Unknown	Unknown

BridgeDTC1	Unknown	Unknown

Tableau 5 : Tableau des Neighbors

Annexe B : Scan des ports avec NMAP

Nmap est un outil d'exploration réseau et scanneur de ports/sécurité dont la syntaxe est la suivante : Nmap [types de scans ...] [options] {spécifications des cibles}. Nmap existe aussi en mode graphique sous le nom « Zenmap GUI ».

Nmap permet d'éviter certaines attaques et aussi de connaître quels services tournent sur une machine. Une installation faite un peu trop vite peut laisser des services en écoute (donc des ports ouverts sans que cela ne soit nécessaire) et donc vulnérables à une attaque.

Nmap est un logiciel très complet et très évolutif, et il est une référence dans le domaine du scanning.

I. Description de NMAP

Nmap a été conçu pour rapidement scanner de grands réseaux, mais il fonctionne aussi très bien sur une cible unique. Nmap innove en utilisant des paquets IP bruts pour déterminer quels sont les hôtes actifs sur le réseau, quels services (y compris le nom de l'application et la version) ces hôtes offrent, quels systèmes d'exploitation (et leurs versions) ils utilisent, quels types de dispositifs de filtrage/pare-feux sont utilisés, ainsi que des douzaines d'autres caractéristiques.

Nmap est généralement utilisé pour les audits de sécurité mais de nombreux gestionnaires des systèmes et de réseau l'apprécient pour des tâches de routine comme les inventaires de réseau, la gestion des mises à jour planifiées ou la surveillance des hôtes et des services actifs.

Le rapport de sortie de Nmap est une liste des cibles scannées ainsi que des informations complémentaires en fonction des options utilisées.

II. Différents types de Scan

Nmap permet d'effectuer des scans en utilisant différents techniques issus de l'étude du comportement des machines respectant le RFC 7932 (TCP). Parmi la douzaine de techniques de scan connues, on peut citer les suivantes :

- **Scan TCP SYN: Le scan SYN est celui par défaut et le plus populaire pour de bonnes raisons. Il peut être exécuté rapidement et scanner des milliers de ports par seconde sur un réseau rapide lorsqu'il n'est pas entravé par des pare-feux. Le scan SYN est relativement discret et furtif, vu qu'il ne termine jamais les connexions TCP. Nmap émet un paquet sur le port ciblé et attend la réponse qui peut être :**
  - Un paquet SYN/ACK qui indique que le port est ouvert ;
  - Un paquet RST qui indique que le port est fermé ;
  - Pas de réponse si le port est filtré.

- **Scan TCP connect : c'est le type de scan par défaut quand le SYN n'est pas utilisable. Tel est le cas lorsque l'utilisateur n'a pas les privilèges pour les paquets bruts (raw packets) ou lors d'un scan de réseaux IPv6. Son exécution est plus lente que le premier et requiert l'option -sT.**

- **Scan UDP : même si les services les plus connus d'Internet sont basés sur le protocole TCP, les services UDP sont aussi largement utilisés. DNS, SNMP ou DHCP (ports 53, 161/162 et 67/68) sont les trois exemples les plus courants. Comme le scan UDP est généralement plus lent et plus difficile que TCP, certains auditeurs de sécurité les ignorent. C'est une erreur, car les services UDP exploitables sont courants et les attaquants eux ne les ignoreront pas. Le scan UDP est activé avec l'option -sU. Il peut être combiné avec un scan TCP, comme le scan SYN (-sS), pour vérifier les deux protocoles lors de la même exécution de Nmap.**

III. Différents états des ports

Nmap retourne les résultats des scans sous forme d'états de ports scannés. Les six états des ports reconnus par Nmap sont :

- ***Ouvert :*** une application accepte des connexions TCP ou des paquets UDP sur ce port.
- ***Fermé :*** le port fermé est accessible (il reçoit et répond aux paquets émis par Nmap), mais il n'y a pas d'application en écoute.
- ***Filtré :*** Nmap ne peut pas toujours déterminer si un port est ouvert car les dispositifs de filtrage des paquets empêchent les paquets de tests (probes) d'atteindre leur port cible.
- ***non-filtré :*** l'état non-filtré signifie qu'un port est accessible, mais que Nmap est incapable de déterminer s'il est ouvert ou fermé.
- ***Ouvert/filtre :*** Nmap met dans cet état les ports dont il est incapable de déterminer l'état entre ouvert et filtré.
- ***Fermé/filtré :*** cet état est utilisé quand Nmap est incapable de déterminer si un port est fermé ou filtré. Cet état est seulement utilisé par le scan Idle basé sur les identifiants de paquets IP.

IV. Le test éffectué

Nous avons utilisé le Scanneur NMAP pour scanner le réseau de DEPC de Marsa Maroc, et indiquer les ports ouverts.

Le résultat de scan effectué pour le serveur Boserver est le suivant :

```
Starting Nmap 5.51 ( http://nmap.org ) at 2011-06-02 16:11 Afr. centrale Ouest
NSE: Loaded 57 scripts for scanning.
Initiating Ping Scan at 16:11
Scanning 172.16.1.241 [4 ports]
Completed Ping Scan at 16:11, 0.84s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:11
Completed Parallel DNS resolution of 1 host. at 16:11, 13.00s elapsed
Initiating SYN Stealth Scan at 16:11
Scanning 172.16.1.241 [1000 ports]
Discovered open port 3389/tcp on 172.16.1.241
Discovered open port 139/tcp on 172.16.1.241
Discovered open port 23/tcp on 172.16.1.241
Discovered open port 445/tcp on 172.16.1.241
Discovered open port 135/tcp on 172.16.1.241
Discovered open port 2383/tcp on 172.16.1.241
Discovered open port 1433/tcp on 172.16.1.241
Discovered open port 1075/tcp on 172.16.1.241
Discovered open port 1080/tcp on 172.16.1.241
Discovered open port 1042/tcp on 172.16.1.241
Discovered open port 1501/tcp on 172.16.1.241
Discovered open port 27000/tcp on 172.16.1.241
Discovered open port 1037/tcp on 172.16.1.241
Completed SYN Stealth Scan at 16:11, 1.22s elapsed (1000 total ports)
Initiating UDP Scan at 16:11
Scanning 172.16.1.241 [1000 ports]
Discovered open port 137/udp on 172.16.1.241
Completed UDP Scan at 16:11, 1.55s elapsed (1000 total ports)
Initiating Service scan at 16:11
Scanning 24 services on 172.16.1.241
Discovered open port 1434/udp on 172.16.1.241
Discovered open|filtered port 1434/udp on 172.16.1.241 is actually open
Service scan Timing: About 45.83% done; ETC: 16:12 (0:00:38 remaining)
Service scan Timing: About 62.50% done; ETC: 16:13 (0:00:47 remaining)
Completed Service scan at 16:13, 129.07s elapsed (24 services on 1 host)
Initiating OS detection (try #1) against 172.16.1.241
Initiating Traceroute at 16:13
Completed Traceroute at 16:13, 0.03s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 16:13
Completed Parallel DNS resolution of 2 hosts. at 16:13, 13.00s elapsed
NSE: Script scanning 172.16.1.241.
Initiating NSE at 16:13
Completed NSE at 16:14, 31.74s elapsed
Nmap scan report for 172.16.1.241
Host is up (0.00s latency).
Not shown: 1976 closed ports
```

```
PORT      STATE        SERVICE       VERSION
23/tcp    open         telnet        Microsoft Windows XP telnetd (no more connections allowed)
135/tcp   open         msrpc         Microsoft Windows RPC
135/tcp   open         msrpc         Microsoft Windows RPC
139/tcp   open         netbios-ssn
445/tcp   open         microsoft-ds  Microsoft Windows 2003 or 2008 microsoft-ds
1037/tcp  open         msrpc         Microsoft Windows RPC
1042/tcp  open         afrog?
1075/tcp  open         msrpc         Microsoft Windows RPC
1080/tcp  open         msrpc         Microsoft Windows RPC
1433/tcp  open         ms-sql-s      Microsoft SQL Server 2000 8.00.766; SP3a
1501/tcp  open         sas-3?
2383/tcp  open         ms-olap4?
3389/tcp  open         microsoft-rdp Microsoft Terminal Service
27000/tcp open         flexlm        FlexLM license manager
123/udp   open|filtered ntp
137/udp   open         netbios-ns    Microsoft Windows NT netbios-ssn (workgroup: INTRA)
138/udp   open|filtered netbios-dgm
445/udp   open|filtered microsoft-ds
500/udp   open|filtered isakmp
1025/udp  open|filtered blackjack
1026/udp  open|filtered win-rpc
1100/udp  open|filtered mctp
1105/udp  open|filtered ftranhc
1434/udp  open         ms-sql-m      Microsoft SQL Server 8.00.194 (ServerName: BOSERVER; TCPPort: 1433).
```

le ré

(les
serv

perr
serv
plus

V. L'intervention effectuée

En vue de sécuriser le réseau DEPC de Marsa Maroc, nous avons pensé à scanner le réseau à l'aide de dispositifs 5View et NMAP, afin de relever les ports utilisés et les ports ouverts non opérationnels.

D'après le résultat obtenu à l'issu de capture de trafic effectué par les deux scanneurs (5View par le tableau xx et le NMAP), on va établir les instructions nécessaires afin de les intégrer au serveur Boserver pour fermer les ports ouverts.

Lexiques

(1) L'adressage IP :

Une **adresse IP** (avec IP pour Internet Protocol) est un numéro d'identification qui est attribué à chaque branchement d'appareil à un réseau informatique utilisant l'Internet Protocol. Il existe des adresses IP de version 4 et de version 6. La version 4 est actuellement la plus utilisée : elle est généralement représentée en notation décimale avec quatre nombres compris entre 0 et 255, séparés par des points, ce qui donne par exemple : 212.85.150.134.

(2) SNMP :

Simple Network Management Protocol (abrégé SNMP), en français « protocole simple de gestion de réseau », est un protocole de communication qui permet aux administrateurs réseau de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseaux et matériels à distance.

(3) Telnet :

Telnet (TErminal NETwork ou TELecommunication NETwork, ou encore TELetype NETwork) est un protocole réseau utilisé sur tout réseau supportant le protocole TCP/IP. Il appartient à la couche session du modèle OSI et à la couche application du modèle ARPA. Il est normalisé par l'IETF (RFC 854 et RFC 855). Selon, l'IETF, le but du protocole Telnet est de fournir un moyen de communication très généraliste, bi-directionnel et orienté octet.

telnet est aussi une commande permettant de créer une session Telnet sur une machine distante. Cette commande a d'abord été disponible sur les systèmes Unix, puis elle est apparue sur la plupart des systèmes d'exploitation. Notez que Telnet est installé mais non activé par défaut sous Microsoft Windows Vista et Microsoft Windows 7.

(4) Switch :

Un **commutateur réseau** (ou **switch**, de l'anglais) est un équipement qui relie plusieurs segments (câbles ou fibres) dans un réseau informatique. Il s'agit le plus souvent d'un boîtier disposant de plusieurs ports Ethernet (entre 4 et plusieurs centaines) . Il a donc la même apparence qu'un concentrateur (hub).

Contrairement à un concentrateur, un commutateur ne reproduit pas sur tous les ports chaque trame qu'il reçoit : il sait déterminer sur quel port il doit envoyer une trame, en fonction de l'adresse à laquelle cette trame est destinée. Les commutateurs sont souvent utilisés pour remplacer des concentrateurs.

(5) Broadcast :

Le broadcast est un terme anglais définissant une diffusion de données à un ensemble de machines connectées à un réseau. En français on utilise le terme diffusion.

(6) Serveur :

Dans un réseau informatique, un **serveur** est à la fois un ensemble de logiciels et l'ordinateur les hébergeant dont le rôle est de répondre de manière automatique à des demandes de services envoyées par des clients — ordinateur et logiciel — via le réseau.

(7) Liaison FO :

Les liaisons Fibres Optiques sont la solution ultime d'interconnexion multisites à grande vitesse (de 2 à 100 Mbs). C'est le produit idéal pour des applications de clients/serveurs gourmandes en volumes et transactions.

(8) Firwall :

Un **pare-feu** (appelé aussi *coupe-feu*, *garde-barrière* ou **firewall** en anglais), est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (notamment internet). Le pare-feu est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseau suivante :

- une interface pour le réseau à protéger (réseau interne) ;
- une interface pour le réseau externe.

(9) Routeur :

Un **routeur** est un élément intermédiaire dans un réseau informatique assurant le routage des paquets. Son rôle est de faire transiter des paquets d'une interface réseau vers une autre, selon un ensemble de règles formant la table de routage. C'est un équipement de couche 3 du modèle OSI.

(10) Liaison FH :

Est une liaison radioélectrique point à point, bi-latérale et permanente (full duplex), à ondes directives, offrant une liaison de bonne qualité et sûre permettant la transmission d'informations en mode multiplex à plus ou moins grande capacité, de 3 à 60 voies

(11) Fédérateur :

Est un type de switchs avec une capacité élevé en terme de nombre de ports

(12) Guest :

Utilisateur Invité

(13) SSH :

Le protocole **SSH** (Secure Shell) a été mis au point en 1995 par le Finlandais Tatu Ylönen.

Il s'agit d'un protocole permettant à un client (un utilisateur ou bien même une machine) d'ouvrir une session interactive sur une machine distante (serveur) afin d'envoyer des commandes ou des fichiers de manière sécurisée :

Les données circulant entre le client et le serveur sont chiffrées, ce qui garantit leur confidentialité (personne d'autre que le serveur ou le client ne peut lire les informations transitant sur le réseau). Il n'est donc pas possible d'écouter le réseau à l'aide d'un analyseur de trames.

(14) AAA :

En sécurité informatique, AAA correspond à un protocole qui réalise trois fonctions : l'authentification, l'autorisation, et la traçabilité (en Anglais : Authentication, Authorization, Accounting/Auditing).

AAA est un modèle de sécurité implémenté dans certains routeurs Cisco mais que l'on peut également utiliser sur toute machine qui peut servir de NAS (*Network Authentification System*).

(15) Nexus :

Nexus est un commutateur ultra-rapide développé par Cisco.

(16) TPS :

Systèmes de detection d'intrusion et systèmes de détection et de prévention de l'intrusion, fournissent un complément technologique aux firewalls en leur permettant une analyse plus intelligente du trafic

Modèle OSI : Les protocoles de réseau sont tous basés sur un ensemble standardisé de fonctionnalités. Cet ensemble a été créé par l'International Standards Organisation (ISO) et est appelé modèle OSI (Open Systems Interconnection) à sept niveaux. Tous les protocoles de réseau s'inscrivent, d'une manière ou d'une autre, dans ce cadre conceptuel. Les couches définies sont : Physique, Liaison de données, Réseau, Transport, Session, Présentation, Application.
Paquet : Groupement logique d'informations qui inclut un en-tête contenant des informations de contrôle et généralement des données utilisateur. Les paquets sont le plus souvent utilisés pour se référer aux unités de données de la couche réseau.
Port : Emplacement sur un commutateur permettant une connexion avec un câble et donc avec l'équipement se trouvant à l'autre extrémité du câble.
Qualité de service (QoS) : Mesure des performances d'un système de transmission qui reflète la qualité et le service offerts. Ensemble des mécanismes permettant de gérer les délais, la latence et la congestion.
Redondance : Duplication d'équipements, de services ou de connexions pour que, dans l'éventualité d'une panne, les dispositifs redondants puissent effectuer le travail de ceux qui sont défaillants.
Commutateur : Elément de réseau qui permet l'envoi, le filtrage et la réexpédition de paquets, en se basant sur l'adresse de destination de chaque paquet. Il opère par défaut au niveau liaison de données (niveau 2 du modèle OSI).
Concentrateur : Généralement, un terme utilisé pour décrire un équipement servant de point central d'une topologie de réseau en étoile et qui connecte des stations terminales. Il opère au niveau physique (niveau 1 du modèle OSI), également appelé « hub ».
Domaine de diffusion « (broadcast domain) » : Ensemble de tous les équipements qui reçoivent les trames diffusées en mode broadcast et émanant de n'importe quel équipement de cet ensemble. Les domaines de diffusion sont généralement limités par les routeurs (ou par des réseaux locaux virtuels sur un réseau commuté), car ceux-ci ne transmettent par les trames envoyées dans ce mode.
Ethernet : Spécification d'un réseau local à bande de base. Les réseaux Ethernet utilisent la technique d'accès au média CSMA/CD et sont exécutés sur de nombrux types de câbles à 10, 100 et 1 000 Mbit/s.