

République Algérienne Démocratique et Populaire  
Ministère de L'enseignement Supérieur et de la Recherche Scientifique  
**Université de Abderrahmane MIRA**  
Faculté des Sciences Exactes  
**Département Informatique**



# Mémoire de Fin de Cycle

En vue de l'obtention du diplôme Master professionnel en  
Informatique

Spécialité : Administration et Sécurité des Réseaux

THÈME

---

Solution de sécurisation des sites distants de l'EPB et  
mise en place d'un système de supervision (open  
source)

---

Réalisé par:

BRAHIMI Yacine  
BOUCHEFA Mehdi

Encadré par :

Dr FARAH Zoubeyr  
Mr BETACHE Idir

Les membres du Jury :

Président: Mr BOUZIDI El Hadi  
Examineur: Mr ALOUI Abdelouahab

Promotion 2014/2015

## REMERCIEMENTS

Nous remercions DIEU pour SA GRÂCE et SA MISÉRICORDE.

Nous tenons à remercier aussi:

- > Nos parents pour leur soutien et leurs efforts quotidiens
- > Notre promoteur Dr FARAH Zoubeyr pour ses conseils et toutes les recommandations qu'il n'a cessé de nous apporter
- > Notre encadreur au sein de l'EPB Mr BETACHE Idir pour son encouragement, son aide et orientation durant la période du projet et aussi tout le personnel du Département Informatique pour leur sympathie.

Enfin, notre profonde gratitude et notre respect à toute personne qui a contribué de près ou de loin à l'élaboration de ce travail.

## DÉDICACES

Nous dédions ce travail :

A nos chers parents pour leur amour, sacrifices et soutiens.

A nos camarades pour leur compréhension et fidélité.

A nos enseignants pour leurs efforts remarquables.

A ceux à qui nous devons reconnaissance.

# Table des matières

Remerciements.....	I
Dédicaces.....	II
Table des matières.....	III
Liste des figures.....	VI
Liste des tableaux.....	VIII
Liste des Acronymes.....	IX

## Introduction

générale.....	1
Partie I.....	2
Chapitre 1: Présentation du cadre de stage.....	2
1.Présentation de la structure d'accueil.....	2
1.1 Missions et activités de l'EPB.....	2
1.1.1 Missions.....	2
1.1.2 Activités.....	3
1.1.3 Présentation des différentes structures de l'entreprise.....	3
1.2 Etude de l'existant.....	4
1.2.1 Le réseau informatique de l'EPB.....	4
1.2.2 L'architecture réseau de l'entreprise.....	5
1.3 Contexte du projet à réaliser.....	6
1.3.1 Présentation du projet.....	6
1.3.2 Diagnostic de la situation du réseau.....	7
1.3.3 Cahier des charges.....	7
1.4 Etude des choix.....	7
1.4.1 Les plates formes de supervisions.....	7
1.4.1.1 Les offres éditeurs.....	7
1.4.1.2 Les offres libres.....	8
1.4.2 Choix du logiciel.....	8
1.5 Conclusion.....	8
Partie II.....	9
Chapitre 1 : Généralités sur les VPNs.....	9
Introduction.....	9
1.1 Principe de fonctionnement des VPNs.....	9
1.2 Les types d'utilisation de VPN.....	10
1.2.1 Le VPN d'accès.....	10
1.2.2 L'intranet VPN.....	11
1.2.3 L'extranet VPN.....	11
1.3 Protocoles utilisés.....	12
1.3.1 PPP (Point to point Protocol).....	12
1.3.2 PPTP (Point to point Tunneling Protocol).....	12
1.3.3 L2F (Layer two Forwarding).....	13
1.3.4 P2TP (Layer 2 Tunneling Protocol).....	13
1.3.5 IPSec (IP security).....	14
1.3.6 MPLS/VPN.....	14
1.3.6.1 Terminologie MPLS.....	15
1.3.6.2 Overlay model.....	16
1.3.6.3 Peer to peer model.....	17
1.3.6.4 Principe de fonctionnement.....	17

1.3.7 Comparaison MPLS/IPSec.....	20
1.4 Conclusion.....	21
Chapitre 2 :Réalisation.....	22
Introduction.....	22
2.1 Présentation du logiciel GNS 3.....	22
2.2 Description de l'architecture.....	23
2.2.1 Technologie utilisé.....	24
2.2.2 Méthodologie d'approche.....	24
2.2.3 L'activation du MPLS.....	24
2.2.4 L'activation du MPLS VPN.....	24
2.3 Configuration d'un VPN MPLS.....	25
2.4 Conclusion.....	35
Partie III.....	36
Chapitre 1 : Présentation de l'outil de supervision Nagios.....	36
1.1 La supervision.....	36
1.1.1 Définition.....	36
1.1.2 Objectifs.....	36
1.1.3 Domaines d'applications.....	36
1.1.4 Pourquoi superviser ?.....	36
1.1.5 Comment superviser ?.....	37
1.2 Le protocole SNMP (Simple Network Management Protocol).....	37
1.3 La MIB (Management Information Base).....	38
1.4 Nagios.....	39
1.4.1 Fonctionnalités.....	40
1.4.2 Architecture.....	41
1.4.3 Plugins.....	41
1.4.4 Les fichiers de configuration.....	43
1.5 Conclusion.....	44
Chapitre 2 : Les complément de nagios.....	45
2.1 NDOutils.....	45
2.1.1 Utilités.....	45
2.1.2 Architecture.....	45
2.2 Centreon.....	46
2.2.1 Utilités.....	47
2.2.2 Architecture.....	47
2.2.2.1 Centreon et Base de données.....	47
2.2.2.2 Centreon et démons.....	47
2.3 NSClient pour la supervision des serveurs Windows .....	49
2.3.1 Architecture.....	49
2.4 NRPE pour la supervision des serveurs Linux .....	50
2.4.1 Architecture.....	50
2.5 Conclusion.....	50
Chapitre 3: Mise en place du système de supervision.....	51
3.1 Environnement de mise en place.....	51
3.1.1 Environnement matériel.....	51
3.1.2 Environnement logiciel.....	51
3.1.3 topologie réseau liée à la supervision de l'EPB.....	52
3.2. Mise en place de Nagios/Centreon et les plugins.....	52
3.2.1 pre-requis Nagios/Centreon.....	52

3.2.2 installation Nagios/Centreon.....	53
3.2.3 Installation de NSClient.....	53
3.2.4 Installation de NRPE.....	53
3.3 Interfaces de Nagios/Centreon.....	53
3.4 Notification par mail.....	56
3.5 Conclusion.....	57
Conclusion General.....	58
Annexe A.....	59
Annexe B.....	73
Annexe C.....	75
Annexe D.....	78
Bibliographie.....	80

---

# Liste des figures

1.1 Organigramme générale de l'EPB.....	3
1.2 Réseau fibre optique de l'EPB.....	4
1.3 Architecture réseau de l'EPB.....	5
Partie I	
2.1 Schéma générique de tunnelisation.....	10
2.2 Le VPN d'accès.....	11
2.3 L'intranet VPN.....	11
2.4 L'extranet VPN.....	12
2.5 Principe d'encapsulation PPTP.....	13
2.6 Principe d'encapsulation L2TP.....	14
2.7 Représentation des VPN/MPLS.....	15
2.8 Overlay model.....	16
2.9 Peer to peer model.....	17
2.10 Principe de fonctionnement(1).....	18
2.11 Principe de fonctionnement(2).....	19
3.1 Maquette réalisée.....	23
3.2 Commande «traceroute» exécutée au niveau du routeur CEB.....	33
3.3 Commande «traceroute» exécutée au niveau du routeur CEA.....	33
3.4 Commande «show ip vrf» exécutée au niveau du router PEB.....	33
3.5 Commande «show ip vrf» exécutée au niveau du router PEA.....	34
3.6 Commande «show mpls forwarding-table» au niveau du routeur PEB.....	34
3.7 Commande «show ip cef vrf epb» au niveau du routeur PEA.....	34
Partie II	
4.1 Echange entre l'agent et manager.....	38
4.2 Arborecence d'une MIB standard.....	38
4.3 Branche internet d'une MIB.....	39
4.4 Centralisation d'information par Nagios.....	40
4.5 Architecture de Nagios.....	41
4.6 Relation entre Nagios et les plugins.....	42
4.7 Principe de fonctionnement des plugins.....	43
5.1 Architecture NDOutils.....	46
5.2 Interaction entre Nagios et Centreon.....	48
5.3 Architecture NSClient.....	49
5.4 Mécanisme du NRPE.....	50

---

6.1 Schéma de la topologie réseau liée à la supervision.....	52
6.2 Interface de vue globale.....	53
6.3 Interface des statistiques Nagios.....	54
6.4 interface de graphiques de performance.....	54
6.5 Interface des hôtes supervisées.....	55
6.6 Interface des services Supervisés.....	55
6.7 Interface des d'évènements.....	56
6.8 Configuration des notifications.....	57
A.1 Page d'accueil de Nagios.....	64
A.2 Host groups.....	65



---

# Liste des Tableaux

Tableau 1.1: Comparaison entre MPLS et IpSec.....	21
Tableau 2.1: Configuration du routeur CEA.....	25
Tableau 2.2: Configuration du routeur PEA.....	28
Tableau 2.3: Configuration du routeur PEB.....	30
Tableau 2.4: Configuration du routeur CEB.....	31
Tableau 2.5: Configuration du routeur P.....	32

---

## Glossaire

### A

**ASIC** Application Specific Interface Circuits

**ATM** Asynchronous transfer mode

### B

**BGP** Border Gateway Protocol

### C

**CEF** Cisco Express Forwarding

### D

**Diffserv** Differentiated Services

**DSCP** Differentiated Services Code Point

### E

**EGP** Exterior Gateway Protocol

**EIGRP** Enhanced Interior Gateway Routing Protocol

### F

**FR** Frame Relay

**FEC** Forwarding Equivalency Class

### G

**GRE** Generic Routing Encapsulation

### I

**IETF** Internet Engineering Task Force

**Intserv** Integrated Services

**IGP** Interior Gateway Protocol

**IGRP** Interior Gateway Routing Protocol

**ISIS** Intermediate System-to-Intermediate System

**ISP** Internet Service Provider

### L

**LDP** Label Distribution Protocol

**LSP** Label Switching Path

**LSR** Label Switching Router

---

## M

**MIB** Management Information Base  
**MPLS** Multi Protocol Label Switching  
**MP-BGP** MultiProtocol-Border Gateway Protocol  
**MTU** Maximum Transmission Unit

## O

**OID** Object Identifier  
**OSPF** Open Shortest Path First

## P

**PDU** Protocol Data Unit  
**PPP** Point to Point Protocol  
**POP** Point of Presence  
**PHP** Penultimate Hop Popping

## Q

**QoS** Quality of Service

## R

**RD** Route distinguishers  
**RIP** Routing Information Protocol  
**RSVP** Ressource Reservation Protocol  
**RT** Route Targets

## S

**SDH** Synchronous Digital Hierarchy  
**SNMP** Simple Network Management Protocol

## T

**TDP** Tag Distribution Protocol  
**TE** Traffic Engineering  
**TTL** Time to Live

## V

**VPN** Virtual private Network  
**VRF** VPNRouting and Forwarding

## W

**WDM** Wavelength Division Multiplexing

---

## Introduction générale

Les réseaux et les systèmes d'informations sont des outils indispensables au fonctionnement des entreprises. Aujourd'hui, ils sont déployés dans des domaines aussi critiques que la sécurité, la santé ou encore les finances. Certaines de ces entreprises peuvent avoir des réseaux qui s'étendent sur de longues distances géographiques. Ces derniers étant au cœur des activités des entreprises et leur maîtrise devient primordiale. Cependant, comme de plus en plus de données sont stockées sur ordinateurs et leur nombre ne cesse de s'accroître. Cette croissance s'accompagne naturellement avec l'augmentation du nombre d'utilisateurs connus ou non, ces utilisateurs n'ayant pas forcément pleins de bonnes intentions vis-à-vis des ces réseaux. Il peuvent exploiter les vulnérabilités de celui-ci pour essayer d'accéder à des informations sensibles afin de les lire, modifier, voir à les détruire pour porter atteinte au bon fonctionnement du système. Il s'avère nécessaire de garantir la sécurité et l'authentification des clients mais aussi surveiller l'état du réseau afin de permettre la disponibilité des ressources, la fiabilité et l'efficacité de ce dernier.

Dès lors que ces réseaux sont très sollicités par les utilisateurs, il est nécessaire de vérifier son état en temps réel en mettant en place un dispositif de surveillance réseau pour nous informer en cas de problèmes. Grâce à un tel système, l'administrateur minimisera le temps d'intervention et les anomalies peuvent être aussitôt résolues avant l'effet domino sur le réseau.

Dans le cadre de notre projet, nous avons choisi de mettre en place deux solutions: d'une part, une infrastructure VPN MPLS en raison des avantages offerts par celle-ci (la sécurité, la gestion de qualité de service pour le traitement de la congestion et la garantie de service) que nous implémenterons à l'aide de l'outil GNS3. D'autre part, la mise en place du système de supervision à base de Nagios et Centreon que nous allons configurer sur une machine virtuelle utilisant le système d'exploitation linux (Debian).

Afin de d'atteindre les objectifs visés, nous avons organisé ce travail en trois parties:

- La première partie est consacrée à la présentation de la structure d'accueil et l'étude de l'existant.
- La deuxième partie est focalisée sur la notion de réseaux privés virtuels (VPNs) : Leur principe de fonctionnement, les différents protocoles et la réalisation d'un VPN MPLS.
- La troisième partie concerne la notion de supervision, les outils et la configuration du système de supervision.

Enfin, nous terminerons par une conclusion générale résumant les éléments essentiels qui ont été abordés dans ce mémoire.

---

## **Partie I**

### **CHAPITRE I: Présentation du cadre du stage**

Ce chapitre se focalise sur la présentation de la structure d'accueil et l'étude détaillée de l'existant où nous cernerons la problématique de notre sujet et nous présenterons la solution adoptée pour ce dernier.

#### **1. Présentation de la structure d'accueil**

Le port de Béjaïa joue un rôle très important dans les transactions internationales vu sa place et sa position géographique.

Aujourd'hui, il est classé 2ème port d'Algérie en marchandises générales et 3ème port pétrolier. Il est également le 1er port du bassin méditerranéen certifié ISO 9001 :2000 pour l'ensemble de ses prestations, et à avoir ainsi installé un système de management de la qualité. Cela constitue une étape dans le processus d'amélioration continue de ses prestations au grand bénéfice de ses clients. L'Entreprise Portuaire a connu d'autres succès depuis, elle est notamment certifiée à la Norme ISO 14001 :2004 et au référentiel OHSAS 18001 :2007, respectivement pour l'environnement et l'hygiène et sécurité au travail.

Le port de Bejaïa, est délimité par :

- 1 - Au nord par la route nationale N°9.
- 2 - Au sud par les jetées de fermeture et du large sur une largeur de 2 750m.
- 3 - A l'est par la jetée Est.
- 4 - A l'ouest par la zone industrielle de Bejaïa

#### **1.1 Missions et activités de l'EPB**

##### **1.1.1 Missions**

La gestion, l'exploitation et le développement du domaine portuaire sont les charges essentielles de la gestion de l'EPB, c'est dans le but de promouvoir les échanges extérieurs du pays.

Elle est chargée des travaux d'entretien, d'aménagement, de renouvellement et de création d'infrastructures.

L'EPB assure également des prestations à caractère commercial, à savoir ; le remorquage, la manutention et l'acconage.

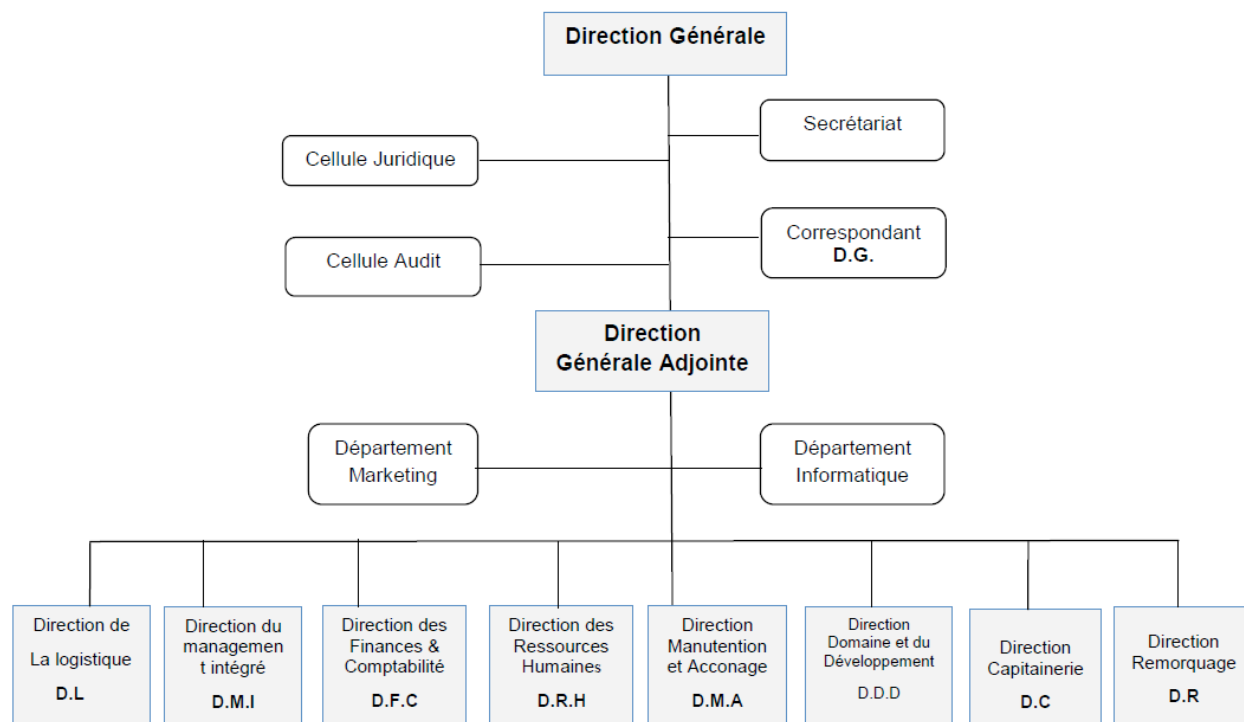
## 1.1.2 Activités

Les principales activités de l'entreprise sont :

- L'exploitation de l'outillage et des installations portuaires.
- L'exécution des travaux d'entretien, d'aménagement et de renouvellement de la super structure portuaire.
- L'exercice du monopole des opérations d'acconage et de manutention portuaire.
- L'exercice du monopole des opérations de remorquage, de pilotage et d'amarrage.
- La police et la sécurité portuaire dans la limite géographique du domaine public portuaire

## 1.1.3 Présentation des différentes structures de l'entreprise

L'EPB est organisée selon l'organigramme général suivant :



**Figure 1.1 : Organigramme général de l'EPB**

## 1.2 Etude de l'existant

### 1.2.1 Le réseau informatique de l'EPB

Le réseau du port de Bejaïa s'étend du port pétrolier (no16) aux ports 13 et 18 (port à bois). La salle machine du réseau local de l'EPB contient principalement une armoire de brassage et une autre armoire optique de grande taille, éventuellement l'ensemble des serveurs, ces deux armoires servent à relier les différents sites de l'entreprise avec le département informatique par des fibres optiques de type 4 et 12 brins.

Chaque site a une armoire de brassage contenant un convertisseur(s) media, un/plusieurs Switch où sont reliés les différents équipements par des câbles informatique.

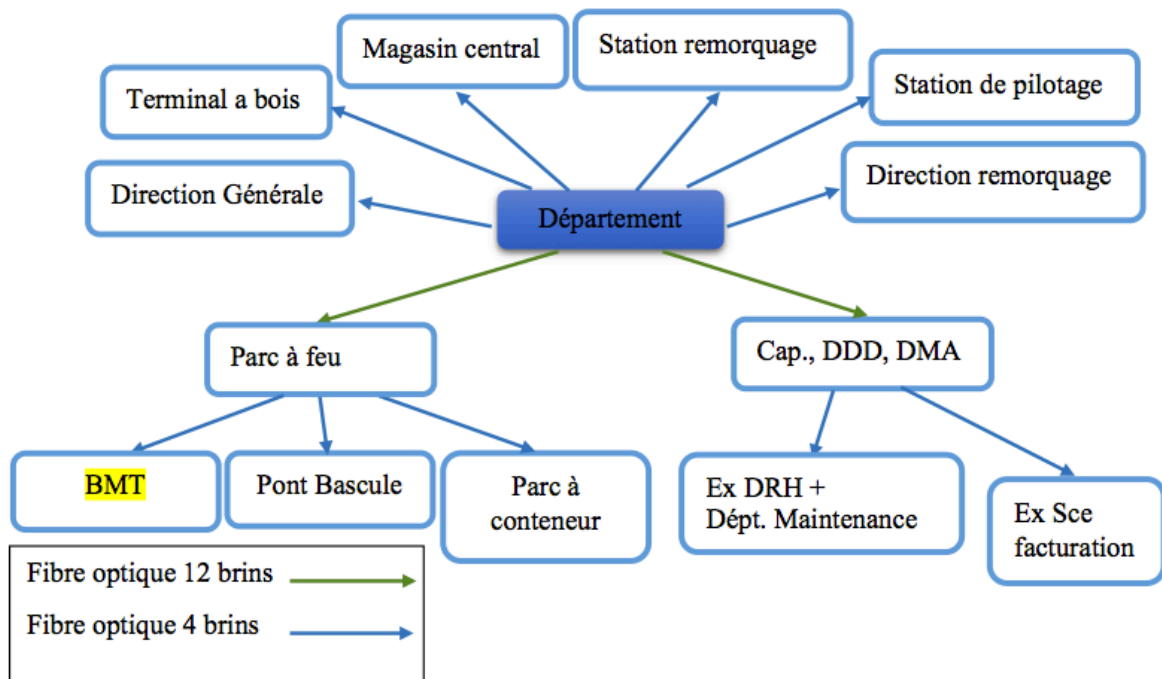
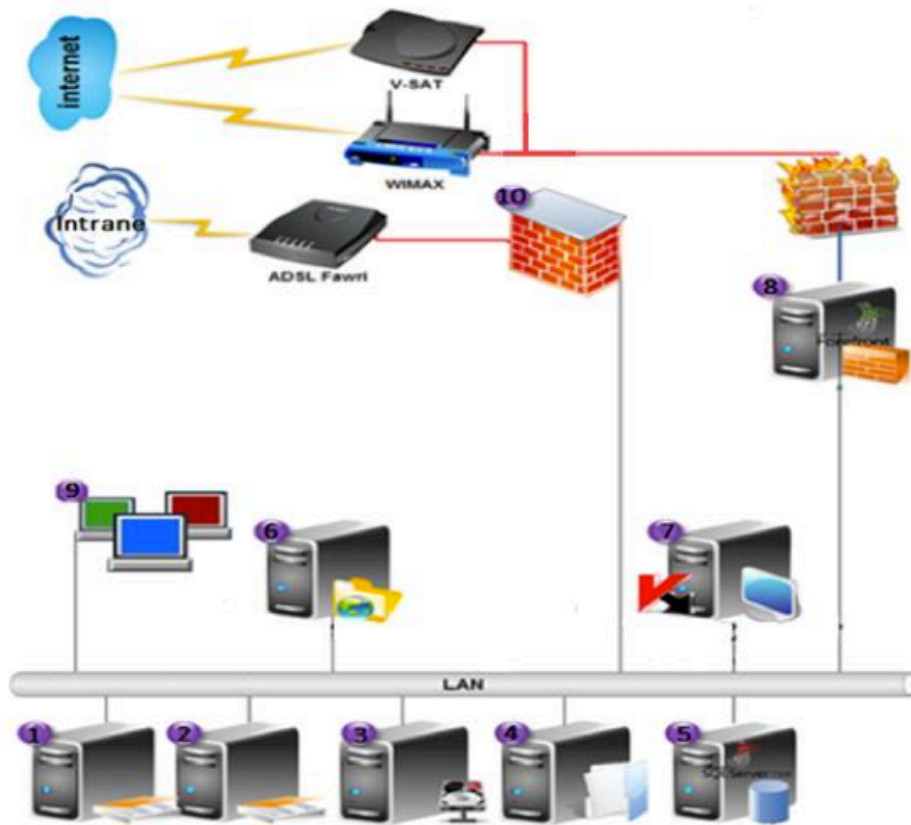


Figure 1.2 : Réseau Fibre Optique de l'EPB

## 1.2.2 L'architecture réseau de l'entreprise

L'architecture réseau du port de Béjaïa est comme la démontre la figure suivante :



**Figure 1.3:**Architecture réseau de l'EPB.

1. Contrôleur du domaine principal (Active Directory) sous Windows server 2003
2. Contrôleur du domaine redondance sous Windows server 2003
3. Serveur de sauvegarde sous Windows server 2003
4. Serveur de fichier sous Windows server 2003
5. Serveur de base de données avec SQL server 2008 R2
6. Serveur d'applications web sous Windows server 2003
7. Serveur sécurité et surveillance et kit d'administration
8. Serveur proxy ISA Server 2006
9. Parc PC
10. Pare feu



---

## • Description du schéma

Le département informatique dispose d'une salle machine contenant principalement de huit machines serveurs, pare-feu et parc PC.

Le réseau de l'entreprise repose sur une architecture client/serveur, qui est centralisée mais on constate le manque d'un routeur, ce qui engendre un vrai problème.

Pour se connecter via le réseau, l'EPB utilise trois types différents de modems : modem ADSL (Asymmetrical Digital Subscriber Line), modem satellite (V-Sat) et un modem WIMAX (Worldwide Interoperability for Microwave Access) pour le réseau Internet en utilisant des pare feu logiciels tel que Isa server 2004 et TMG 2010 mais aussi sans l'utilisation de pare feu matériel qui assure plus de sécurité.

L'EPB se base sur l'utilisation des produits Microsoft sous licence. Elle utilise comme système d'exploitation pour les ordinateurs : Windows XP et Seven mais pour les serveurs : Windows Server 2003 qui ne répond plus aux nouveaux besoins.

Les différents équipements sont reliés grâce à des switch Catalyst 2950 de CISCO.

### 1.3 Contexte du projet à réaliser

Dans cette partie, nous allons en premier lieu présenter le projet à réaliser, suivi des objectifs issus de l'achèvement de ce dernier, en second lieu nous allons dégager la problématique associée au cahier de charges de l'organisme.

#### 1.3.1 Présentation du projet

Le projet à réaliser, s'intitule «Solution de sécurisation des sites distants de l'EPB et mise en place d'un système de supervision» .

La mise en œuvre de ce projet permet d'apporter des améliorations au réseau de l'entreprise, en mettant l'accent sur la supervision et une meilleure sécurité de ce dernier en utilisant des liaisons VPNs.

Donc, notre tâche consiste, à garantir une meilleure exploitation et attribution du réseau ainsi à assurer une communication sûre et confidentielle entre les utilisateurs au sein de l'entreprise.

---

## 1.3.2 Diagnostic de la situation du réseau

L'étude que nous avons menée, nous a permis de soulever d'autres faiblesses réseaux existantes dans l'entreprise et qui sont les suivantes :

- Incapacité de vérifier la disponibilité et de déterminer la qualité de service des serveurs
- Incapacité de détecter la défaillance des équipements (charge CPU, Etat mémoire, surcharge du disque...).
- Manque de liaisons sécurisées entre les plates-formes extra-portuaires.

## 1.3.3 Cahier des charges

- Améliorer la sécurité entre les quatre plates-formes reliées à l'EPB par la créations de liaisons VPN.
- Mise en place d'un système de supervision.

## 1.4 Etude de choix

De nombreuses plateformes de supervision existent aujourd'hui. L'analyse des différentes solutions de supervision nous a conduit à choisir NAGIOS par rapport à sa réputation, sa communauté et sa flexibilité.

De même pour les réseaux VPNs, il existe plusieurs solutions, que ce soit des solutions logicielles, matérielles ou des solutions clés en main, chacune de ces solutions a ses avantages et inconvénients. Dans ce qui suit, nous citerons quelques unes de ces solutions.

### 1.4.1 Les plateformes de supervisions

#### 1.4.1.1 Les offres éditeurs

Vu que le marché de la supervision est en plein expansion, de nombreuses sociétés investissent dans des produits permettant d'assurer une meilleure gestion des réseaux. Parmi ces solutions nous avons:

- HP Open View
- IBM Tivoli monitoring
- Microsoft System Center

==> Ces solutions sont trop coûteuses.

#### 1.4.1.2 Les offres libres

Il existe des solutions de supervision libres et professionnelles. Parmi les plus répandues, reconnues du moment nous pouvons citer:

- Nagios
- Zabbix
- Munin

- 
- OpenNMS.

L'avantage de ces logiciels libres est la gratuité, la disponibilité du code source et la liberté d'étudier et de modifier le code selon nos besoins et de le diffuser. De plus, il existe une communauté importante d'utilisateurs et de développeurs qui participent à l'amélioration des logiciels et apportent une assistance par la mise en ligne des documentations et les participations aux forums.

### **1.4.2 Choix du logiciel**

Parmi les solutions les plus connues, recommandées et surtout libres, on citera Nagios. Cette solution libre est plus répandue et plus utilisée. Par rapport à notre projet, Nagios est plus adaptée et répondait pratiquement à tous les besoins organisationnels et financiers de la société.

De plus Nagios est une solution stable, dispose d'une grande communauté de développeurs et est utilisée aussi bien dans les petites et moyennes infrastructures que dans les grands parcs informatiques et utilisée surtout par plusieurs entreprises de renommé, tels que Yahoo (100 000 serveurs), Yellow pipe Web Hosting (7000 serveurs) ...

Bien que ce dernier soit réputé par sa configuration complexe et fastidieuse, couplé à Centreon un logiciel qui lui servira de couche applicative afin de faciliter la configuration et d'établir des interfaces IHM plus ergonomiques et compréhensibles.

## **1.5 Conclusion**

À travers ce chapitre, nous avons présenté la structure d'accueil et l'architecture réseau dont elle dispose. Après une étude de l'existant et sa critique, nous avons soulevé quelques problèmes rencontrés par la société ce qui nous a permis de cerner la problématique de notre projet.

Dans les parties suivantes, nous allons détailler les solutions proposées et leurs utilités.

---

## Partie II

### Chapitre 1: Généralités sur les VPNs

#### Introduction

Actuellement, les réseaux sont au coeur des activités au sein des entreprises et certaines d'entre elles disposent de parcs informatiques de plus en plus importants qui comportent des applications et des données essentielles à l'entreprise.

La sécurité des réseaux et la confidentialité des données constituent un sujet important qui favorise des échanges d'information dans tous les domaines.

Le problème qui se pose est le suivant: Comment relier les différents pôles d'une entreprise alors qu'ils sont répartis sur de grandes distances géographiques tout en assurant la sécurité et l'accès aux données de ces clients ?

Pour remédier à ce problème, ces entreprises mettent en place des réseaux VPN.

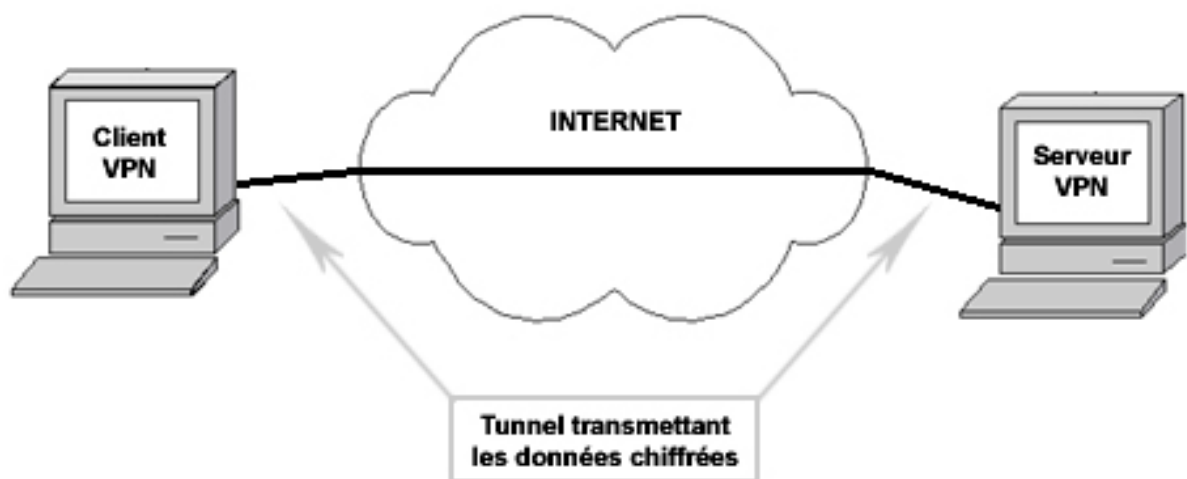
Nous verrons dans ce mémoire le principe de fonctionnement du VPN ainsi que les différents types d'utilisation du VPN et les protocoles de la mise en place de ce dernier.

#### 1.1 Principe de fonctionnement des VPNs

Un réseaux VPN reposent sur un protocole nommé « protocole de tunneling », (ou encore protocoles de tunnelisation). Il permet d'acheminer les informations de l'entreprise de façon cryptée d'un bout à l'autre du tunnel en utilisant les algorithmes de cryptographie .

Le principe de tunnelling consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Par la suite, la source chiffre les données et les achemine en empruntant ce chemin virtuel.

Afin d'assurer un accès aisé et peu coûteux aux intranets ou aux extranets d'entreprise, les réseaux VPN d'accès simulent un réseau privé, alors qu'ils utilisent en réalité une infrastructure d'accès partagée comme internet. Les données à transmettre peuvent être prises en charge par un protocole différent d'IP. Dans ce cas, le protocole de tunneling encapsule les données en ajoutant un en-tête. Le tunneling est l'ensemble des processus d'encapsulation, de transmission et de dés-encapsulation [1].



**Figure 2.1:**Schéma générique de Tunnelisation

## 1.2 Les types d'utilisation de VPN

Il existe 3 types standards d'utilisation des VPNs à savoir[1]:

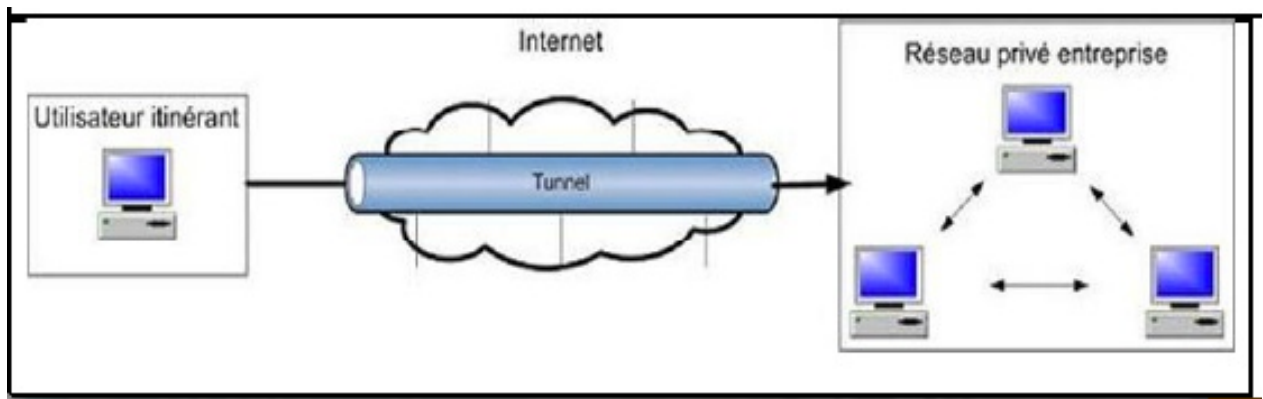
- Le VPN d'accès
- L'intranet VPN
- L'extranet VPN

### 1.2.1 Le VPN d'accès(Host to Lan)

Le VPN d'accès est utilisé pour permettre à des utilisateurs itinérants d'accéder au réseau privé de leur entreprise. L'utilisateur se sert de sa connexion Internet pour établir la connexion VPN.

On a deux cas :

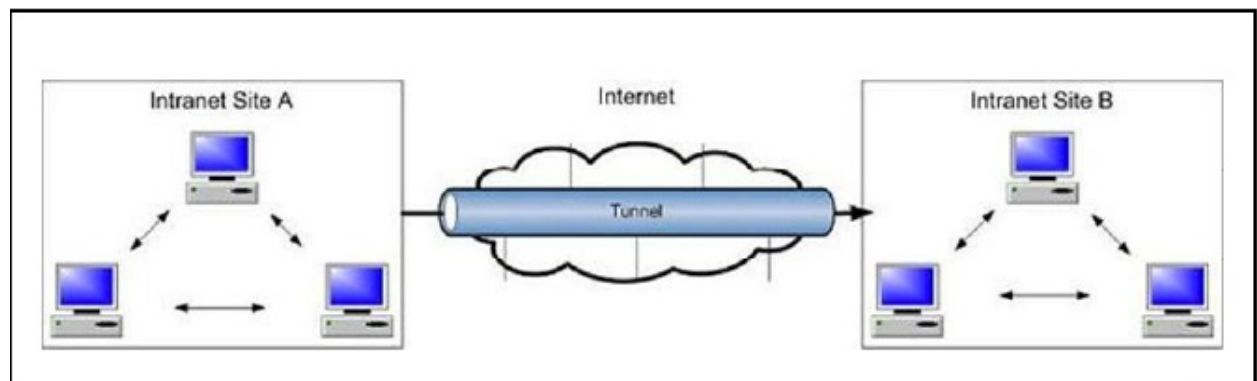
- L'utilisateur demande au fournisseur d'accès de lui établir une connexion cryptée vers le serveur distant : il communique avec le NAS (Network Access Server) du fournisseur d'accès et c'est le NAS qui établit la connexion cryptée.
- L'utilisateur possède son propre logiciel client pour le VPN auquel cas il établit directement la communication de manière cryptée vers le réseau de l'entreprise.



**Figure 2.2:** Le VPN d'accès

### 1.2.2 L'intranet VPN(LAN to LAN)

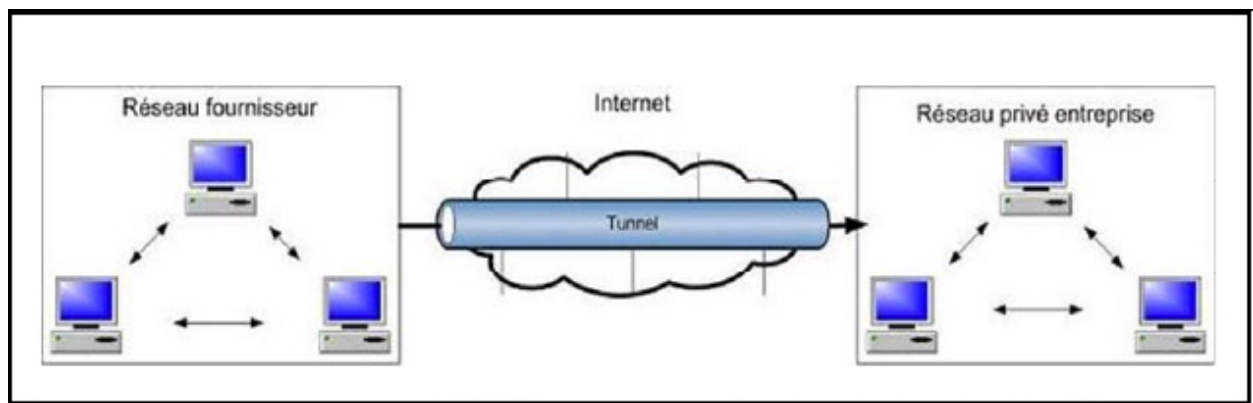
L'intranet VPN est utilisé pour relier au moins deux intranets entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants. Le plus important dans ce type de réseau est de garantir la sécurité et l'intégrité des données.



**Figure 2.3:** L'intranet VPN

### 1.2.3 L'extranet VPN

Une entreprise peut utiliser le VPN pour communiquer avec ses clients et ses partenaires. Elle ouvre alors son réseau local à ces derniers. Dans Ce cadre, il est fondamental que l'administrateur du VPN puisse tracer les clients sur le réseau et gérer les droits de chacun sur celui-ci.



**Figure 2.4:**L'extranet VPN

### 1.3 Protocoles utilisés

Il existe plusieurs protocoles de tunnelisation qui permettent la création des réseaux VPN. Les technologies les plus utilisées pour la création de tunnels sécurisés pour tout type de flux sont PPP, PPTP, L2F, L2TP et IPSec [2].

#### 1.3.1 PPP (Point to Point Protocol)

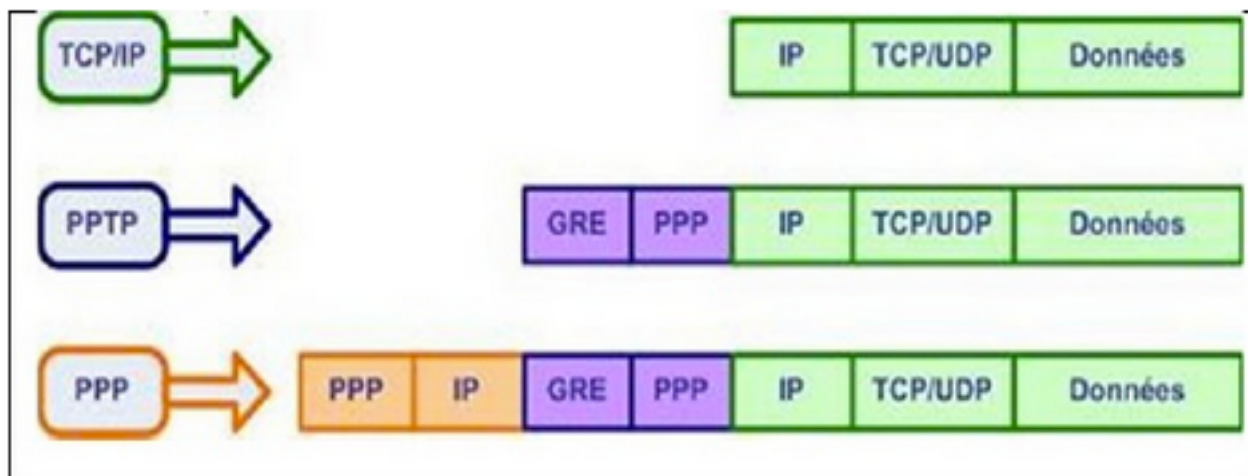
C'est un ensemble de protocoles standard garantissant l'interopérabilité des logiciels d'accès distant de divers éditeurs, il permet de transférer des données sur un lien synchrone ou asynchrone, il est full duplex, garantit l'ordre d'arrivée des paquets et encapsule les paquets IP, IPX dans des trames PPP; puis les transmet au travers des liaisons point à point [2].

#### 1.3.2 PPTP (Point to Point Tunneling Protocol)

PPTP est un protocole réseau permettant un transfert sécurisé entre un client distant et un serveur privé. Ceci est réalisé à l'aide d'un VPN basé sur TCP/IP. La technologie utilisée est une extension du protocole PPP permettant l'accès à distance. Les différents rôles que le protocole PPTP peut assurer sont listés ci-dessous [2]:

1. Permet la création des VPN sur demande sur des réseaux basés sur TCP/IP.
2. Peut être utilisé sur un même réseau local entre deux machines.
3. Peut être utilisé comme support pour la création de VPN aussi bien Internet que le réseau téléphonique public.
4. Offre une communication encryptée sûre à travers ces réseaux publics.
5. Simplifie les accès longues distances pour les utilisateurs distants.

la figure 1.5 modélise le principe d'encapsulation PPTP.



**Figure 2.5:**Principe d'encapsulation PPTP

### 1.3.3 L2F (Layer Two Forwarding)

L2F est un protocole de niveau 2 du modèle OSI qui permet à un serveur distant de véhiculer le trafic sur PPP et de transférer ces données jusqu'au serveur L2F(routeur). Ce serveur L2F dés-encapsule les paquets et les envoie sur le réseau. Il faut noter que contrairement à PPTP et L2TP, L2F n'a pas besoin de client [3].

### 1.3.4 L2TP (Layer Two Tunneling Protocol)

Le protocole L2TP est issu de la convergence des protocoles PPTP et L2F. Ainsi le protocole L2TP encapsule des trames PPP, encapsulant elles-mêmes d'autres protocoles tels que IP mais aussi IPX ou encore NetBIOS. Lorsqu'il est configuré pour transporter les données sur IP, L2TP peut être utilisé pour faire du tunnelling sur Internet.

L2TP repose sur deux concepts [2]:

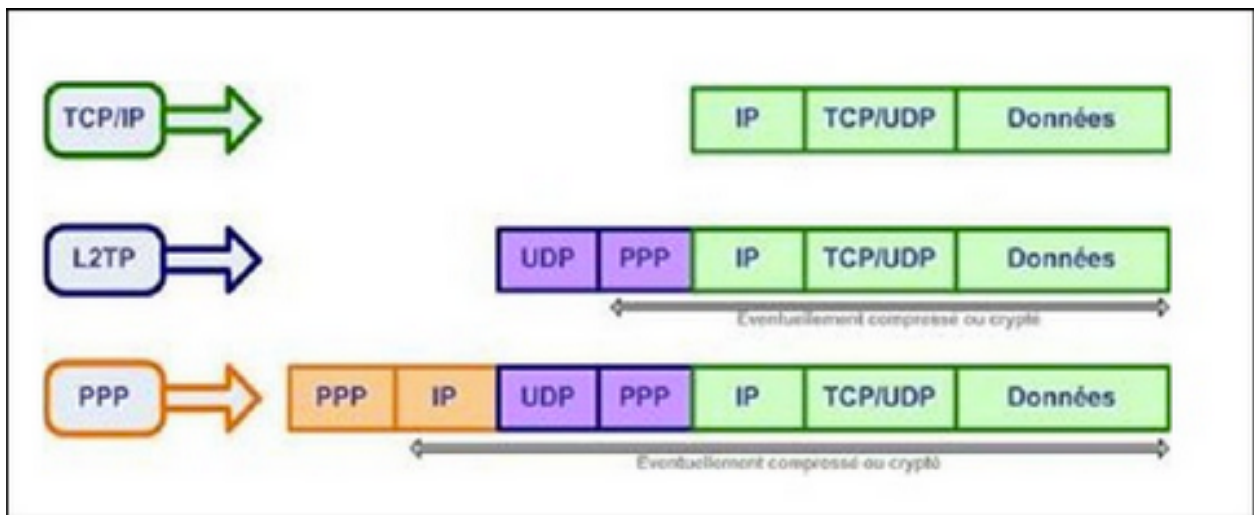
- les concentrateurs d'accès L2TP (LAC) : Ces périphériques LAC fournissent un support physique aux connexions L2TP. Le trafic étant alors transféré sur les serveurs réseau L2TP. Ces serveurs peuvent s'intégrer à la structure d'un réseau commuté RTC ou alors à un système d'extrémité PPP prenant en charge le protocole L2TP. Ils assurent le fractionnement en canaux de tous les protocoles basés sur PPP. Le LAC est l'émetteur des appels entrants et le destinataire des appels sortants.
- les serveurs réseau L2TP (LNS) : Le LNS gère le protocole L2TP côté serveur. Le protocole L2tp n'utilise qu'un seul support, sur lequel arrivent les canaux L2TP. Ils sont cependant capables de terminer les appels en provenance de n'importe quelle interface PPP du concentrateur d'accès Lac.

Le LNS est l'émetteur des appels sortants et le destinataire des appels entrants. C'est lui qui sera responsable de l'authentification du tunnel. L2TP n'intègre pas directement de protocole pour le chiffrement des données. C'est pourquoi on l'utilise très souvent avec le protocole IPSec.



On distingue principalement 2 composantes dans les paquets L2TP :

- Les paquets d'information, encapsulés dans des paquets PPP pour les sessions utilisateurs qui servent pour le transport de L2TP.
- Le protocole de signalisation, qui utilise le contrôle de l'information L2TP est encapsulé dans des paquets UDP/IP.



**Figure 2.6:** Principe d'encapsulation L2T

### 1.3.5 IPSec (IP Security)

IPSec est un protocole qui permet de sécuriser les échanges au niveau de la couche réseau. Il s'agit en fait d'un protocole apportant des améliorations au niveau de la sécurité au protocole IP afin de garantir la confidentialité, l'intégrité et l'authentification des échanges.

Le protocole IPSec est basé sur trois modules [2]:

- Le premier, Authentication Header (AH) vise à assurer l'intégrité et l'authenticité des datagrammes IP. Il ne fournit, par contre, aucune confidentialité.
- Le second, Encapsulating Security Payload (ESP) peut aussi permettre l'authentification des données mais est principalement utilisé pour le cryptage des informations. Ces deux premiers mécanismes sont presque toujours utilisés conjointement.
- Le troisième, Internet Key Exchange (IKE) permet de gérer les échanges ou les associations entre protocoles de sécurité.

Le protocole IPSec est souvent utilisé avec le L2TP.

### 1.3.6 MPLS/VPN

C'est un mécanisme de transport de données opérant sur la couche de liaison de données du modèle OSI, donc en dessous des protocoles comme IP. Il a été conçu pour fournir un service unifié de transport de données pour les clients en utilisant une technique de commutation de paquets.

MPLS peut être utilisé pour transporter pratiquement tout type de trafic (voix, des paquets IP, etc...).

Ils sont essentiellement implémentés chez les opérateurs. Les opérateurs utilisent leurs backbones sur MPLS pour créer des VPN, par conséquent le réseau MPLS des opérateurs se trouve partagé ou mutualisé avec d'autres clients.

Grâce à l'étanchéité des VPN MPLS, le client aura l'impression de bénéficier d'un réseau qui lui est entièrement dédié tandis que celui-ci possède plusieurs VPNs sur son réseau.

Voici une représentation des VPN/MPLS [4].

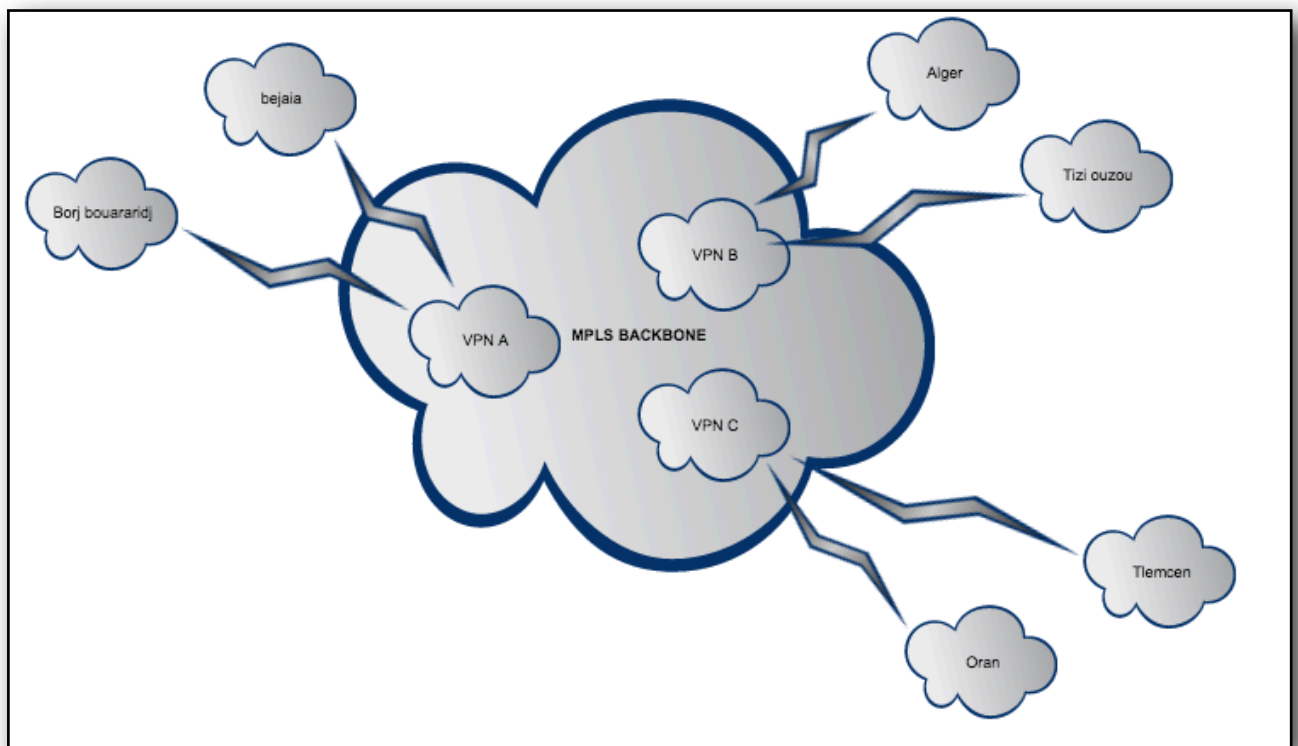


Figure 2.7: Représentation des VPN/MPLS.

#### 1.3.6.1 Terminologie MPLS [5]

- **Label Switch Router : LSR**

- Equipement capable de 'forwarder' :

- des paquets IP natifs,
- des paquets MPLS en utilisant le 'label swapping'.

- Equipement exécute :

- un ou plusieurs protocoles de routage IP (IGP, EGP).
- un protocole de contrôle MPLS.

- **Ingress LSR ('head-end LSR') - ingress LER**

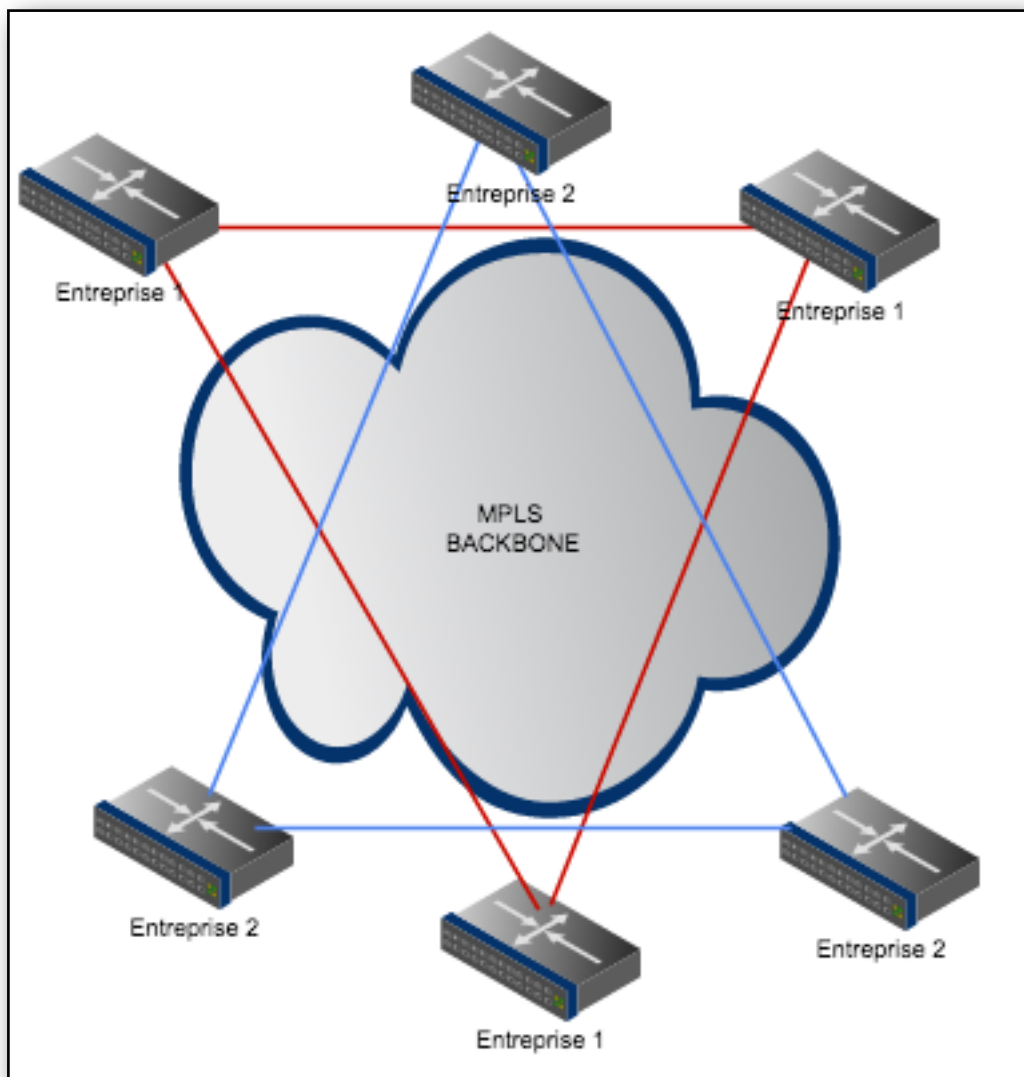
- Génère un en-tête MPLS comportant un label initial à partir du paquet IP arrivant dans le domaine MPLS.

- **Egress LSR ('tail-end LSR') - egress LER**
  - Retire l'en-tête MPLS.

### 1.3.6.2 Overlay model (Modèle de recouvrement)

Le modèle VPN de recouvrement est le plus facile à comprendre, car il permet une séparation très nette entre le client et de responsabilités du fournisseur de services [6]:

Le fournisseur de services fournit au client un ensemble de lignes louées émules. Ces lignes louées sont appelés VCs, qui peut être soit constamment disponible (PVC) ou établies à la demande (SVC). La figure 7-5 illustre la topologie d'un échantillon superposition VPN et les VCs utilisés en elle. Le client établit une communication de routeur à routeur entre le Customer Premises Equipment (CPE) sur les dispositifs VCs fournis par le prestataire de service. Les données de protocole de routage est toujours échangées entre les dispositifs client et le fournisseur de services n'a pas connaissance de la structure interne du réseau du client.



**Figure 2.8:** Overlay model

Bien qu'il soit relativement facile à comprendre et à mettre en œuvre, le modèle VPN de recouvrement a néanmoins un certain nombre d'inconvénients:

Il est bien adapté à des configurations non redondantes avec quelques sites centraux et de nombreux sites distants, mais devient extrêmement difficile à gérer dans une configuration plus maillée.

### 1.3.6.3 Peer to peer model

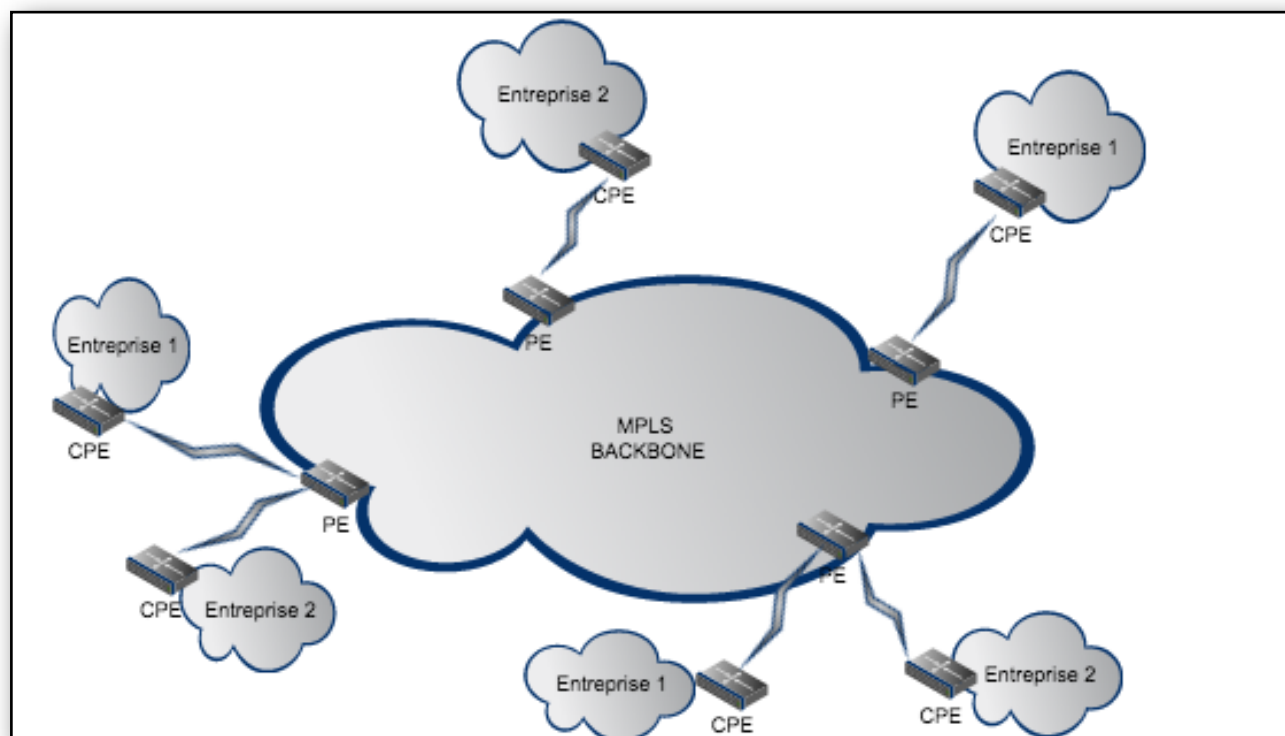


Figure 2.9:Peer to peer model

Dans l'approche de peer to peer, plusieurs clients peuvent être connectés au même routeur PE. Les listes d'accès doivent être configurés sur chaque interface PE-CE sur le routeur PE pour assurer l'isolation entre les clients VPN, pour empêcher un client VPN de pénétrer dans un autre réseau VPN, ou pour empêcher un client VPN d'exécuter d'un déni de service et attaquer un client sur un autre VPN.

De manière générale, la topologie utilisée pour relier les sites dans un VPN avec ce modèle est la topologie entièrement maillée ou «full mesh». Cela implique que tous les sites peuvent se voir ou bien qu'il existe une liaison point à point entre tous les sites du VPN [6].

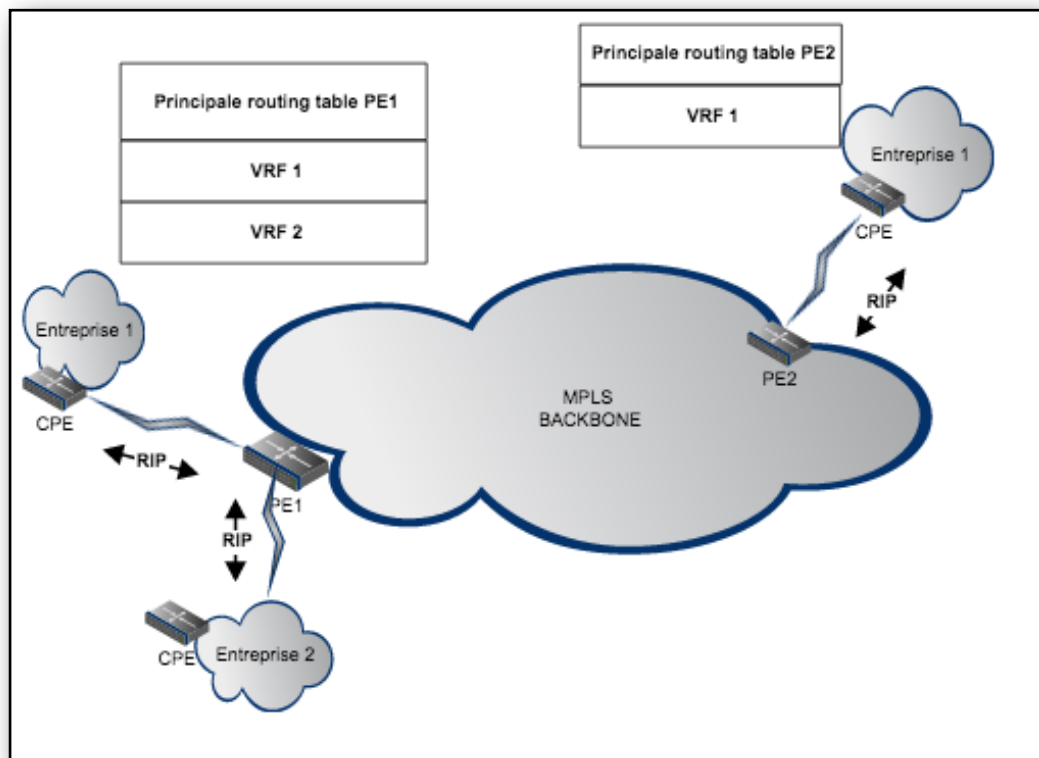
### 1.3.6.4 Principe de fonctionnement

Lors de la conception d'un réseau d'entreprise, les administrateurs choisissent généralement des plages d'adresses IP privées pour leur réseau LAN (10.0.0.0, 172.16.0.0, 192.168.0.0). Or le réseau MPLS permet l'implémentation de plusieurs VPN clients au sein de son réseau. Par conséquent, il est essentiel de trouver un moyen de différencier les adresse de chaque client . La notion de «route distinguisher» ou RD fût alors introduite afin de résoudre ce problème. Cette RD possède une taille de 8 octets et est ajoutée au préfixe ipv4 (de 4 octets) pour étendre l'adressage IP. La taille de cette nouvelle adresse est de 96 bits. Son format est comme suit : RD: préfixe IPV4

Cette extension de l'adresse IP nous permet de différencier les différentes plages d'adresses, elle nous permet également de différencier les VPNs.

De plus, pour rendre la communication inter VPN interdite, la technologie MPLS implémente des tables de routages spécifiques à chaque VPN. Ces tables de routage appelées VRF (Virtual Routing and Forwarding table) se réfèrent aux identifiants de chaque VPN, les RD. De cette façon chaque VPN possèdent leur propre table de routage ou VRF dans le réseau MPLS et ne voient pas les autres routes accessibles sur le réseau MPLS.

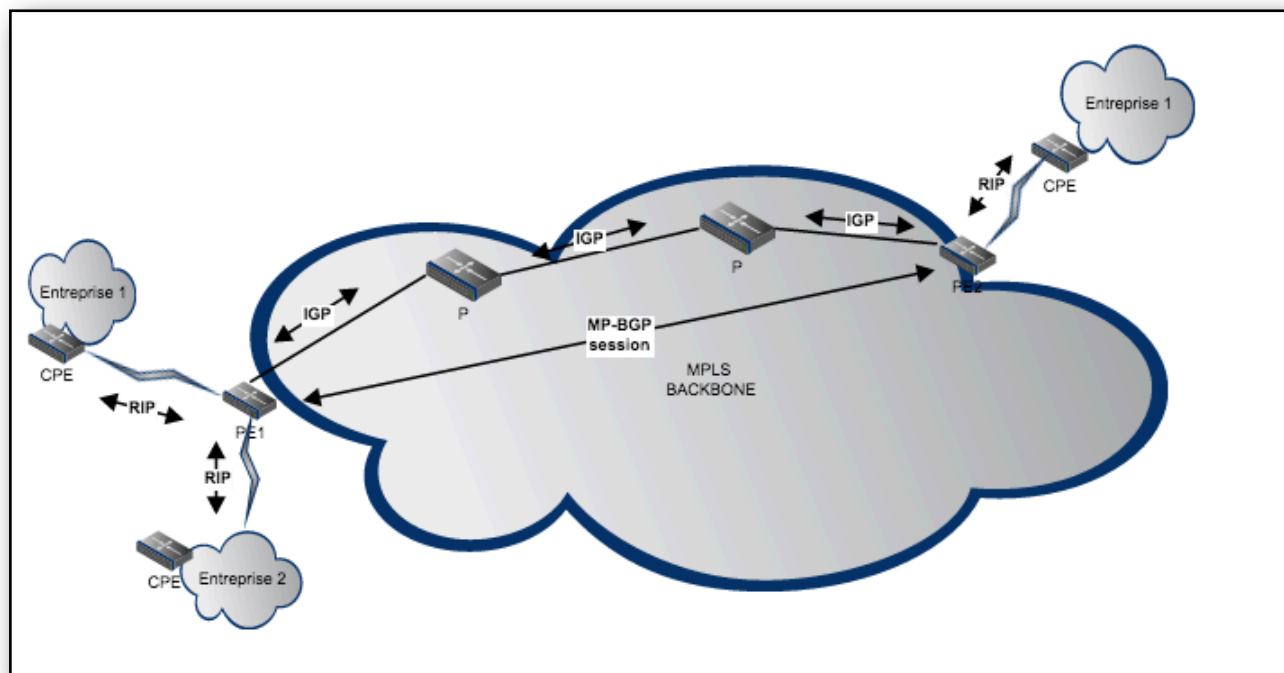
Pour rappel, cette table de routage principale sert à atteindre les autres nœuds LSR au sein du réseau MPLS. Elle est remplie par un protocole de routage IGP et sert à mettre à jour la LFIB qui fait la correspondance entre les FEC et les labels [7].



**Figure 2.10:**Principe de fonctionnement(1)

Sur la figure précédente les sites connectés au VPN matérialisant la connexion CPE-PE peuvent communiquer avec l'intermédiaire d'une route statique ou encore RIP v2, OSPF, BGP... pour envoyer leurs informations vers le PE de l'opérateur. Dans notre exemple nous utilisons le protocole RIP. Lorsqu'un paquet arrive dans un réseau MPLS la notion de pile de labels ou «stack label» intervient. En fonction de la FEC auquel appartient le paquet, l'ingress node consulte sa table de commutation et affecte un label au paquet, et le transmet au LSR suivant. Le label dont vous venons de parler juste avant est déjà inséré sur les paquets, il nous sert à identifier vers quel VPN nous devons communiquer. Lorsque le paquet MPLS arrive sur un LSR interne du nuage MPLS, le protocole de routage fonctionnant sur cet équipement détermine dans la base de données des labels LIB (Label Base Information), le prochain label à appliquer à ce paquet pour qu'il parvienne jusqu'à sa destination. L'équipement procède ensuite à une mise à jour de l'en-tête MPLS (swapping du label et mise à jour du champ TTL, du bit S), avant de l'envoyer au noeud suivant (LSR ou l'egress node). Il faut bien noter que sur un LSR interne, le protocole de routage de la couche réseau n'est jamais sollicité.

Enfin, une fois que le paquet MPLS arrive à l'égress node, l'équipement lui retire toute trace MPLS et le transmet à la couche réseau. Ces données sont finalement envoyées vers le CPE relié au VPN identifié juste avant



**Figure 2.11 :** Principe de fonctionnement(2)

Lorsqu'un PE apprend une nouvelle route:

- Il insère dans sa VRF et indique qu'il sait la joindre en RIP.
- Ensuite il annonce cette route avec les autres PE en établissant une session BGP en fournissant le label associé pour pouvoir atteindre ce VPN en question.
- Enfin, seuls les PE sur lesquels les VRF ont été configurées vont rajouter ces routes dans leur table de routage.

Lorsqu'un paquet de donnée arrive sur un routeur CE, celui-ci regarde la route IPv4 correspondant à l'adresse du site distant, et transmet ce paquet au routeur PE correspondant (sachant qu'un CE peut être attaché à plusieurs PE). Le PE va ensuite router ce paquet vers le PE du site de destination en l'envoyant sur l'interface correspondante. Un label MPLS va alors être apposé au paquet correspondant au chemin de l'interface de sortie selon du routeur PE selon les correspondances établies dans la table de FEC. Le paquet va alors transiter sur le backbone du FA : il va être commuté par les routeurs P. Ceux-ci vont utiliser leur tables FIB pour « swapper » les labels MPLS correspondants à leurs interfaces, jusqu'à arriver au routeur PE de destination. Ce routeur va décapsuler le dernier label MPLS présent, puis transmettre le paquet au CE correspondant (ils peuvent être plusieurs à être connectés au PE). Le CE va ensuite transmettre ce paquet à la destination finale. [7].

**Remarque:** Il se peut que des PE se situent dans le même LAN et que pour envoyer les données du site 1 vers le site 2 ils n'aient pas besoin de passer par un P router. Le transfert se fait alors de PE à PE directement car il s'agit du chemin optimal. Ce procédé est le «Penultimate Hop Popping» qui consiste à retirer des labels avant l'envoi des données vers le nœud egress (PE). Cela évite qu'il ait à consulter 2 fois les labels et l'entête IP de destination pour forwarder les données utilisateurs.

### 1.3.7 Comparaison entre MPLS et IPSec [8]

	MPLS	IpSec
<b>Qualité de service</b>	permet d'attribuer des priorités au trafic par le biais de classes de service.	Le transfert se faisant sur l'internet public, permet seulement un service 'best effort'.
<b>Coût</b>	Inférieur à celui des réseaux Frame Relay et ATM mais supérieur à celui des autres VPN IP.	Faible grâce au transfert via le domaine Internet public.
<b>Sécurité</b>	Comparable à la sécurité offerte par les réseaux ATM et Frame Relay existants.	Sécurité totale grâce à la combinaison de certificats numériques et de PKI pour l'authentification ainsi qu'à une série d'options de cryptage, triple DES et AES notamment.
<b>Applications compatibles</b>	Toutes les applications y compris les logiciels d'entreprise vitaux exigeant une qualité de service élevée et une faible latence et les applications en temps réel (video et voix sur IP).	Accès à distance et nomade sécurisé, Applications sous IP notamment courrier électronique et internet. Inadapté au trafic en temps réel ou à priorité élevée.
<b>Etendue</b>	Dépend du réseau MPLS du fournisseur de service.	Très vaste puisque il repose sur l'accès à internet.
<b>Evolutivité</b>	Évolutivité élevée puisque n'exige pas une interconnexion d'égal à égal entre les sites et que les déploiement standard peuvent prendre en charge plusieurs dizaines de milliers de connexions par VPN.	Les déploiements les plus vastes exigent une planification soigneuse pour répondre notamment aux problèmes d'interconnexion site à site et de peering.

	<b>MPLS</b>	<b>IpSec</b>
<b>Frais de gestion du réseau</b>	Aucun traitement exigé par le routage.	Traitements supplémentaires pour le cryptage et le décryptage.
<b>Vitesse de déploiement</b>	Le fournisseur de service doit déployer un routeur MPLS en bordure de réseau pour permettre l'accès client.	Possibilité d'utiliser l'infrastructure du réseau IP existant.
<b>Prise en charge par le client</b>	Non requise, le MPLS est une technologie réseau.	Logiciels ou matériels client requis.

**Tableau 1.1:** Comparaison entre MPLS et IPsec

## 1.4 Conclusion

Tout au long de ce chapitre, nous avons effectué une présentation des réseaux privés virtuels (VPNs) ainsi que les différents protocoles utilisés pour les réaliser. Le chapitre suivant, sera consacré à la réalisation de l'architecture réseau de l'EPB et sa configuration.



---

## Chapitre2: Réalisation

Nous avons réalisé une maquette simulant la solution MPLS VPN à l'aide de l'émulateur GNS3 de Cisco, une étude a été entamée concernant les différents protocoles de routages et leur configuration sur les routeurs Cisco.

### 2.1 Présentation du logiciel GNS3

a) **Définition:** GNS3 signifie Graphical Network Simulator, c'est un simulateur graphique de réseaux qui permet l'émulation de réseaux complexes. Il est utilisé pour reproduire différents systèmes d'exploitation dans un environnement virtuel. Il permet l'émulation en exécutant un IOS Cisco (Internetwork Operating Systems)[9].

#### b) Les composants du logiciel

Afin de fournir une simulation précise et complète, GNS3 est fortement lié à :

- **Dynamips:** Emulation d'IOS Cisco.
- **Dynagen:** Interface écrite en python et permettant l'interconnexion de plusieurs machines émulées.
- **Qemu:** Emulateur de système.
- **Virtualbox:** Logiciel permettant la création de machines virtuelles.
- **Wireshark:** est un logiciel pour analyser les trames.

Grâce à ces composants, GNS3 nous permet:

- Le design de topologies réseaux de haute qualité et complexe.
- Emulation de plusieurs plate-formes de routeurs Cisco IOS, ou encore IPS, PIX et firewalls ASA.
- Simulation de switches Ethernet, ATM et Frame Relay.
- Connexion de réseaux simulés au monde réel.
- Capture de paquets grâce à Wireshark.

## 2.2 Description de l'architecture

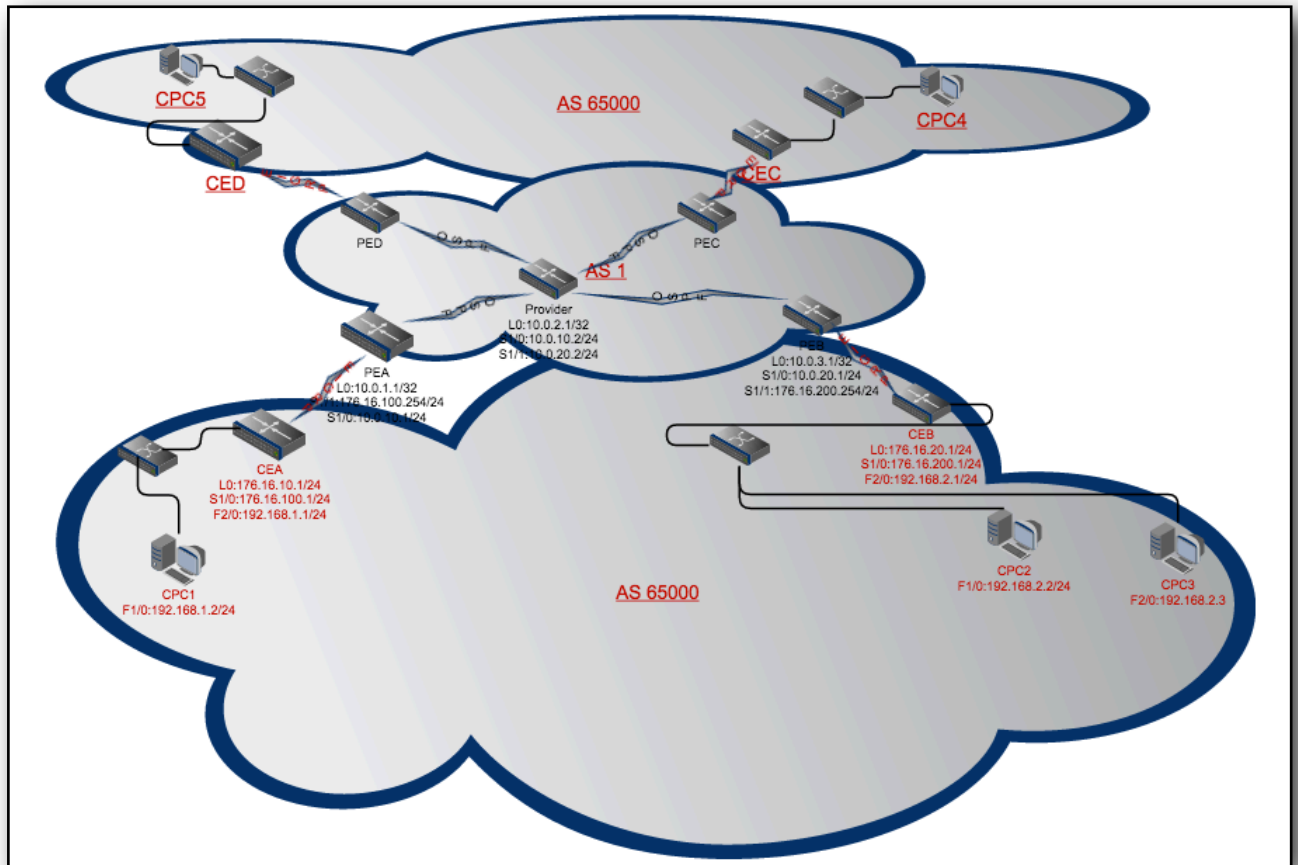


Figure 3.1: Maquette réalisée.

Cette topologie met en évidence un VPN d' Intranet simple entre quatre sites appartenant au client EPB : site A, site B, site C et D. Le réseau du client comprend les routeurs CEA , CEB, CEC et CED. Nous avons utilisé pour cette tâche 9 routeurs dont :

- 1 routeurs représentant le core MPLS (des routeurs P).
- 4 routeurs représentant l'edge MPLS (des routeurs PE) et simulant les routeurs de Béjaia, Adoudaou, El Kseur et Borj bouaararij.
- 4 routeurs clients désignant des sites de l'EPB (des routeurs CE).

Tous les routeurs sont de type Cisco, la gamme 7200 utilisant comme imageIOS «c7200-jk9o3s-mz.124-19.bin » supportant la technologie MPLS.

---

## 2.2.1 Technologies utilisées

Nous avons choisis, pour cette solution, les technologies suivantes:

- **OSPF** pour la communication intra-nuage.
- **EIGRP** en guise de protocole CE-PE.
- **MP-BGP** pour le VPN.

## 2.2.2 Méthodologie d'approche

Après plusieurs recherches sur internet, nous avons remarqué que chaque personne a une certaine méthode qui lui est personnelle, cependant nous avons opté pour la plus aboutis à savoir **[10]**:

1. Configuration des interfaces
2. Mise en place du protocole intra-nuage
3. Mise en place des VRF sur les PE
4. Implémentation du protocole CE-PE
5. Mise en place du protocole MP-BGP
6. Gestion de la redistribution respective des préfixes

## 2.2.3 L'activation du routage MPLS

Nous allons implémenter le protocole OSPF pour garantir la communication intra-nuage des routeurs P et PE , l'utilisation du protocole OSPF n'est pas obligatoire et n'a aucun effet sur le comportement des routeurs. La configuration du protocole BGP en le PE et le CE peut se faire de différentes manières, comme l'utilisation des méthodes de réflecteur de route ou de confédération. Nous allons utiliser la méthode de configuration de voisinage directe qui est la plus simple et moins évolutive. Enfin nous utiliserons MP-BGP entre les routeurs PE. **[11]**.

## 2.2.4 L'activation du MPLS

Nous allons activer Le LDP sur les interfaces qui auront à faire du label switching (les interfaces qui sont dans le backbone MPLS). Les routeurs PE et P supportent MPLS donc l'activation est réalisée à ce niveau. Avant de configurer MPLS sur les interfaces des routeurs, il est indispensable d'activer le CEF (Cisco Express Forwarding) **[12]**.

---

## 2.3 Configuration du VPN MPLS

Cette partie décrit les configurations génériques exigées sur les routeurs dans le domaine du fournisseur de services, pour mettre en application un VPN basé sur MPLS [10]. Toutes les configurations décrites dans les sections suivantes sont exécutées à partir du réseau montré dans la figure 2.1

<b>Hostname CEA</b>	Activation du MPLS
<b>Ip cef</b>	
<b>interface loopback 0</b> <b>ip address 176.16.10.1 255.255.255.0</b>	Configuration de l'interface loopback0
<b>interface fastethernet 2/0</b> <b>ip address 192.168.1.1 255.255.255.0</b>	Configuration de l'interface Fa 2/0
<b>interface serial 1/0</b> <b>ip address 176.16.100.1 255.255.255.0</b>	Configuration de l'interface Se 1/0
<b>router eigrp 65000</b> <b>no auto-summary</b> <b>network 172.16.0.0</b> <b>network 192.168.1.0</b>	Configuration du routage EIGRP entre le routeur CEA et PEA

**Tableau 2.1: Configuration du routeur CEA**

<b>Hostname PEA</b>	Activation du MPLS
<b>Ip cef</b>	
<b>interface loopback 0</b> <b>ip address 10.0.1.1 255.255.255.255</b>	Configuration de l'interface loopback0
<b>interface serial 1/0</b> <b>ip address 10.0.10.1 255.255.255.0</b>	Configuration de l'interface Se 1/0
<b>interface serial 1/1</b> <b>ip address 176.16.100.254 255.255.255.0</b> <b>no shutdown</b>	Configuration de l'interface Se 1/1
<b>router ospf 1</b> <b>network 10.0.0.0 0.255.255.255 area 0</b>	Configuration du routage OSPF entre les routeurs PE
<b>mpls ldp advertise-labels</b> <b>mpls ldp router-id loopback 0 force</b> <b>interface serial 1/0</b> <b>mpls ip</b>	configuration du MPLS IP  (sur les interfaces internes des routeurs opérateurs).

<pre> <b>ip vrf EPB</b>  <b>rd 65000:123</b>  <b>route-target both 65000:123</b> </pre>	<p><b>configurer la VRF sur le routeur PEA:</b> la VRF epb sur le routeur PEA et PEB. Ceci a comme conséquence la création d'une table de routage VRF et d'une table EPB Express Forwarding(CEF) pour EPB. Cet exemple montre EPB VRF étant configuré sur le routeur PEA. Notez que le nom VRF est sensible à la casse.</p> <p><b>Configurer le RD:</b> le RD crée des tables de routage et de transmission. Le RD est ajouté au début des en-têtes IPv4 du client pour les convertir en préfixes globalement uniques VPNv4.</p> <p><b>Configuration des paramètres VRF:RT</b></p> <p>configure l'importation et l'exportation de stratégies pour les communautés MP-BGP. la stratégie est employée pour filtrer des itinéraires pour ce «target-route» particulier.</p>
<pre> <b>interface serial 1/1</b>  <b>ip vrf forwarding EPB</b>  <b>ip address 176.16.100.254 255.255.255.0</b>  <b>no shutdown</b> </pre>	<p>Associer VRF avec une interface.</p> <p>Association de VRP à l'adresse IP de l'interface.</p> <p>Affecter l'adresse après la VRF</p>
<pre> <b>router eigrp 1</b>  <b>address-family ipv4 vrf EPB</b>  <b>autonomous-system 65000</b>  <b>no auto-summary</b>  <b>network 176.16.0.0</b> </pre>	<p>Configuration du routage EIGRP</p>

<b>router bgp 1</b>	Configuration des voisins MP-iBGP.
<b>neighbor 10.0.3.1 remote-as 1</b>	
<b>neighbor 10.0.3.1 update-source loopback 0</b>	Utiliser l'adresse loopback comme adresse source.
<b>address-family vpnv4</b>	Configuration de l'address-family BBGP VPNv4
<b>neighbor 10.0.3.1 activate</b>	
<b>neighbor 10.0.3.1 send-community both</b>	Activer les familles d'adresses IPv4 et vpnv4.
<b>exit</b>	
<b>address-family ipv4 vrf EPB</b>	
<b>redistribute eigrp 65000</b>	Configuration de BGP par VRF IPv4 (contexte de routage).
<b>exit</b>	
<b>exit</b>	
<b>router eigrp 1</b>	
<b>address-family ipv4 vrf EPB</b>	
<b>redistribute bgp 1 metric 64 1000 255 1 1500</b>	

**Tableau 2.2: Configuration du routeur PEA**

<b>Hostname PEB</b>	Activation du MPLS
<b>Ip cef</b>	
<b>interface loopback 0</b> <b>ip address 10.0.3.1 255.255.255.255</b>	Configuration de l'interface loopback0
<b>interface serial 1/0</b> <b>ip address 10.0.20.1 255.255.255.0</b>	Configuration de l'interface Se 1/0
<b>interface serial 1/1</b> <b>ip address 176.16.200.254 255.255.255.0</b> <b>no shutdown</b>	Configuration de l'interface Se 1/1
<b>router ospf 1</b> <b>network 10.0.0.0 0.255.255.255 area 0</b>	Configuration du routage OSPF sur le routeur PEB
<b>mpls ldp advertise-labels</b> <b>mpls ldp router-id loopback 0 force</b> <b>interface serial 1/0</b> <b>mpls ip</b>	Configuration du MPLS
<b>ip vrf EPB</b> <b>rd 65000:123</b> <b>route-target both 65000:123</b>	Configuration de la VRF du routeur PEB
<b>interface serial 1/1</b> <b>ip vrf forwarding EPB</b> <b>ip address 176.16.200.254 255.255.255.0</b> <b>no shutdown</b>	Définition des interfaces dans la VRF



<pre> <b>router eigrp 1</b>  <b>address-family ipv4 vrf EPB</b>  <b>autonomous-system 65000</b>  <b>no auto-summary</b>  <b>network 176.16.0.0</b> </pre>	<p>Configuration du routage EIGRP</p>
<pre> <b>router bgp 1</b>  <b>neighbor 10.0.1.1 remote-as 1</b>  <b>neighbor 10.0.1.1 update-source loopback 0</b>  <b>address-family vpnv4</b>  <b>neighbor 10.0.1.1 activate</b>  <b>neighbor 10.0.1.1 send-community both</b>  <b>exit</b>  <b>address-family ipv4 vrf EPB</b>  <b>redistribute eigrp 65000</b>  <b>exit</b>  <b>exit</b>  <b>router eigrp 1</b>  <b>address-family ipv4 vrf EPB</b>  <b>redistribute bgp 1 metric 64 1000 255 1 1500</b> </pre>	<p>Configuration du protocole BGP</p>

**Tableau 2.3: Configuration du routeur PEB**

<b>Hostname CEB</b>	Activation du MPLS
<b>Ip cef</b>	
<b>interface loopback 0</b> <b>ip address 176.16.20.1 255.255.255.0</b>	Configuration de l'interface loopback0
<b>interface fastethernet 2/0</b> <b>ip address 192.168.2.1 255.255.255.0</b>	Configuration de l'interface Fa 2/0
<b>interface serial 1/0</b> <b>ip address 176.16.200.1 255.255.255.0</b>	Configuration de l'interface Se 1/0
<b>router eigrp 65000</b> <b>no auto-summary</b> <b>network 172.16.0.0</b> <b>network 192.168.2.0</b>	Configuration du routage EIGRP sur le routeur CEB

**Tableau 2.4: Configuration du routeur CEB**

<b>Hostname P</b>	Activation du MPLS
<b>Ip cef</b>	
<b>interface loopback 100</b> <b>ip address 10.0.2.1 255.255.255.255</b>	Configuration de l'interface loopback
<b>interface serial 1/0</b> <b>ip address 10.0.10.2 255.255.255.0</b>	Configuration de l'interface Se 1/0
<b>interface serial 1/1</b> <b>ip address 10.0.20.2 255.255.255.0</b>	Configuration de l'interface Se 1/1
<b>router ospf 1</b> <b>network 10.0.0.0 0.255.255.255 area 0</b>	Configuration du routage ospf
<b>mpls ldp advertise-labels</b> <b>mpls ldp router -id loopback 100 force</b> <b>interface se 1/0</b> <b>mpls ip</b> <b>interface serial 1/1</b> <b>mpls ip</b>	Configuration du routage mpls

**Tableau 2.5: Configuration du routeur P.**

**Verification:**

- **show ip vrf:** Vérifie l'existence de la table VFR.
- **show ip vrf interfaces:** Vérifie les interfaces actives.
- **show ip route vrf EPB:** Vérifie les informations de routage au niveau du routeur PE.
- **traceroute vrf EPB 10.0.0.1:** Vérifie les informations de routage au niveau du routeur PE.
- **show ip bgp vpnv4 tag:** Vérifie le protocole de routage BGP.
- **show ip cef vrf EPB 10.0.0.1 detail:** Vérifie les informations de routage au niveau du routeur PE.

```

CEB#traceroute 192.168.1.1

Type escape sequence to abort.
Tracing the route to 192.168.1.1

 1 176.16.200.254 48 msec 16 msec 12 msec
 2 10.0.20.2 [MPLS: Labels 16/21 Exp 0] 88 msec 88 msec 84 msec
 3 176.16.100.254 [MPLS: Label 21 Exp 0] 52 msec 64 msec 64 msec
 4 176.16.100.1 112 msec * 76 msec

```

**Figure 3.2:** Commande «traceroute» exécutée au niveau du routeur CEB avec l'adresse 192.168.1.1.

Le routeur PEB a inséré 2 Labels dans le paquet, le premier label (21) pour le VPN «EPB», le deuxième label (16) pour la commutation LSP au sein du nuage MPLS. Le routeur P a supprimé le Label (16) du paquet avant de le réexpédier au routeur PEA.

```

CE1#traceroute 192.168.2.1

Type escape sequence to abort.
Tracing the route to 192.168.2.1

 1 176.16.100.254 32 msec 64 msec 8 msec
 2 10.0.10.2 [MPLS: Labels 17/21 Exp 0] 140 msec 72 msec 76 msec
 3 176.16.200.254 [MPLS: Label 21 Exp 0] 76 msec 68 msec 64 msec
 4 176.16.200.1 68 msec * 100 msec

```

**Figure 3.3:** Commande «traceroute» exécutée au niveau du routeur CEA avec l'adresse 192.168.2.1.

Le routeur PEA a inséré 2 Labels dans le paquet, le premier label (21) pour le VPN «EPB», le deuxième label (17) pour le routeur lui-même. Le routeur Pa supprimé le Label(17)du paquet avant de le réexpédier au routeur PEB.

```

PEB#sh ip vrf

```

Name	Default RD	Interfaces
EPB	65000:123	Se1/1

**Figure 3.4:** Commande «Show ip vrf» exécutée au niveau du routeur PEB.

La commande «Show ip vrf» permet de tester l'existence des VRFs sur l'ensemble des interfaces d'un routeur et les afficher.

Dans notre exemple, le nom du vrf est 'EPB' sur l'interface série 1/1.

```
PEA#sh ip vrf int
Interface          IP-Address      VRF              Protocol
Se1/1              176.16.100.254 EPB              up
PEA#
```

**Figure 3.5:** Commande «Show ip vrf interfaces» exécutée au niveau du routeur PEA.

Cette commande permet d'afficher l'interface sur laquelle le VRF est activé, ici c'est l'interface Série 1/1 avec comme adresse IP: 176.16.100.254

```
bilel — Dynamips(4): R3, Console port — telnet — 80x11
PEB#sh mpls forwarding-table
Local  Outgoing  Prefix          Bytes tag  Outgoing  Next Hop
tag    tag or VC  or Tunnel Id    switched   interface
16     16         10.0.1.1/32     0          Se1/0     point2point
17     Pop tag    10.0.2.1/32     0          Se1/0     point2point
18     Pop tag    10.0.10.0/24    0          Se1/0     point2point
19     Untagged  176.16.20.0/24[V] 0          Se1/1     point2point
20     Aggregate 176.16.200.0/24[V] \
                                           0
21     Untagged  192.168.2.0/24[V] 0          Se1/1     point2point
PEB#
```

**Figure 3.6:** Commande «Show mpls forwarding-table» exécutée au niveau du routeur PEB.

Cette commande permet de voir le LFIB de PEB constitué dynamiquement grâce au protocole LDP.

```
bilel — Dynamips(3): R2, Console port — telnet — 80x11
PEA#show ip cef vrf EPB 192.168.2.1
192.168.2.0/24, version 13, epoch 0, cached adjacency to Serial1/0
0 packets, 0 bytes
  tag information set
    local tag: VPN-route-head
    fast tag rewrite with Se1/0, point2point, tags imposed: {17 21}
    via 10.0.3.1, 0 dependencies, recursive
    next hop 10.0.10.2, Serial1/0 via 10.0.3.1/32
    valid cached adjacency
    tag rewrite with Se1/0, point2point, tags imposed: {17 21}
PEA#
```

**Figure 3.7:** Commande «Show ip cef vrf EPB192.168.2.1» exécutée au niveau du routeur PEA.

Cette commande permet d'afficher la table CEF de la vrf EPB.

---

## 2.4 Conclusion

Dans ce chapitre, nous avons, en premier lieu, présenté l'émulateur GNS3 de CISCO. Il est à signaler que la manipulation de ce logiciel est un peu complexe, malgré les difficultés rencontrées nous avons pu parvenir à utiliser un IOS (Image Shell des routeurs CISCO) récent en s'appuyant sur plusieurs recherches ainsi qu'une documentation généralement rédigée en langue anglaise.

En dernier, nous avons choisi une topologie réseau permettant de mettre en œuvre les principales fonctionnalités VPN MPLS. Une topologie qui consiste à interconnecter les quatre sites de l'EPB via un réseau opérateur utilisant comme technologie de transport MPLS. Les résultats obtenus montrent bien le fonctionnement de notre réseau.

---

## Partie III

### Chapitre 1: Présentation de l'outil de supervision Nagios

Dans ce présent chapitre, nous allons définir le concept de supervision et ses objectifs ensuite, nous nous pencherons sur les fonctionnalités de la solution proposée, son architecture, et les différents services qu'elle offre et une présentation des différents fichiers de configuration.

#### 1.1 La supervision [13]

La supervision de réseaux peut être définie comme l'utilisation de ressources réseaux adaptées dans le but de collecter des informations (en temps réel ou non) sur l'utilisation ou l'état des réseaux et de leurs éléments afin d'assurer une haute disponibilité et une répartition optimale de ceux-ci.

##### 1.1.1 Objectifs

Nous pouvons donc résumer l'objectif d'une supervision en trois points :

- Etre réactif en alertant l'administrateur en cas de dysfonctionnement d'une partie du système d'information.
- Etre pro actif en anticipant les incidents possibles.
- Cibler le problème.

##### 1.1.2 Domaines d'applications

La supervision réseaux inclut plusieurs domaines à savoir:

- **Supervision des équipements :**
  - Switchs, routeurs, serveurs, imprimantes, ...etc.
- **Supervision système :**
  - RAM, processeurs, espaces de stockage, ...etc.
- **Supervision des applications :**
  - Disponibilités, compatibilités, performances.

Ceci à travers plusieurs activités comme :

- **La surveillance.**
- **L'analyse.**
- **Le pilotage.**

##### 1.1.4 Pourquoi superviser?

Un parc informatique, en général, est doté de machines fonctionnant sous Linux, Windows ou Mac OS ainsi que de switches, routeur,..etc, il est important de pouvoir donner en temps réel, l'état de celui-ci et de ses constituants afin de pouvoir être avisé en cas de problème et intervenir sur celui-ci . Ceci apparaît comme un véritable outil d'administration et d'aide à la décision.

---

### 1.1.5 Comment superviser?

Il existe différentes manières de superviser parmi lesquelles :

- **L'analyse des fichiers journaux:** Ceux-ci contiennent toutes les informations sur les événements produits sur le système. les fichiers de log sont hébergés dans /var/log/.
- **L'analyse des résultats des commandes et/ou scripts:** L'usage de certaines commandes permet de comprendre les dysfonctionnements d'un équipement. Par exemple, la commande ping 192.168.1.4 permet de savoir si l'équipement d'adresse 192.168.1.4 est joignable ou pas.
- **Profiter des fonctionnalités du SNMP:** SNMP pour Simple Network Management Protocol est un protocole de communication qui permet de gérer les équipements réseaux.

### 1.2 Le protocole SNMP (Simple Network Management Protocole)

Le Simple Network Management Protocol ou SNMP est un protocole de la couche application du modèle OSI. Il offre diverses possibilités de management d'un équipement réseau [1].

Il est utilisé pour la gestion de réseaux. Basé sur le protocole UDP, ce protocole de communication permet la remontée d'informations stockées dans la table MIB ("Management Information Base") des machines. SNMP se base sur une architecture client (Nagios) / serveur (la machine à surveiller).

L'architecture de gestion du réseau proposée par le protocole SNMP est basée sur trois principaux éléments [23] :

- **Les équipements managés (managed devices):** Ce sont des éléments du réseau (ponts, hubs, routeurs ou serveurs), contenant des «objets de gestion» (managed objects) pouvant être des informations sur le matériel, des éléments de configuration ou des informations statistiques.
- **Les agents:** C'est une application de gestion de réseau résidant dans un périphérique et chargée de transmettre les données locales de gestion du périphérique au format SNMP.
- **Les systèmes de management de réseau (network management systems noté NMS):** C'est une console au travers de laquelle les administrateurs peuvent réaliser des tâches d'administration.

Les informations entre l'agent et le superviseur se font avec les cinq commandes suivantes :

- Get-request (GET) pour obtenir la valeur d'un objet de la MIB d'un agent .
- Get-next-request (GETNEXT) pour obtenir la valeur courante du prochain objet .
- Set-request (SET) pour mettre à jour la valeur courante d'un objet de la MIB .
- Get-response renvoie la valeur d'un objet de la MIB .
- Trap (TRAP) signal émis par un agent vers le superviseur.



Le superviseur et l'agent écoutent respectivement sur le port 162 et 161 et le schéma ci-dessous l'illustre bien.

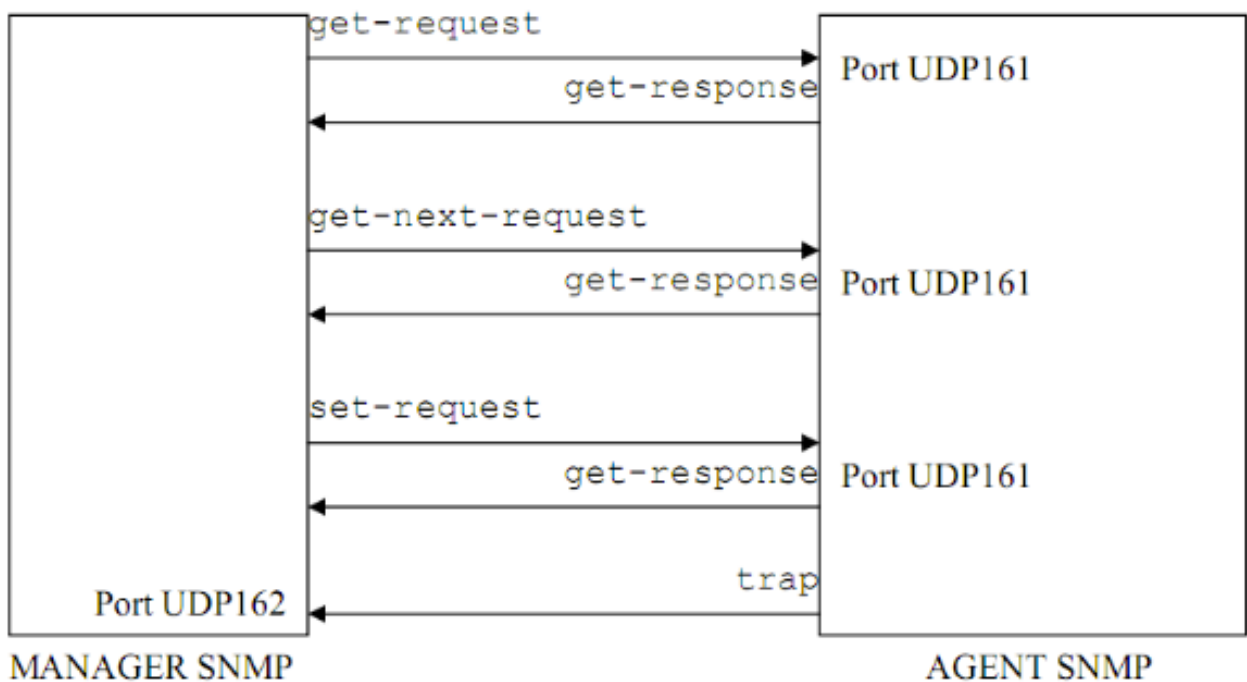


Figure 4.1: Echange entre l'agent et le manager

### 1.3 La MIB (Management Information Base)

La MIB ou Management Information Base est une base de données résidente chez l'agent SNMP. c'est une structure arborescente dont chaque noeud est défini par un nombre ou OID (Object Identifier). Elle contient en général une partie commune à tous les agents SNMP d'un même type de matériel et une partie spécifique à chaque constructeur. Chaque équipement à superviser possède sa propre MIB. c'est une structure normalisée [1]. Une MIB ressemble à ceci :

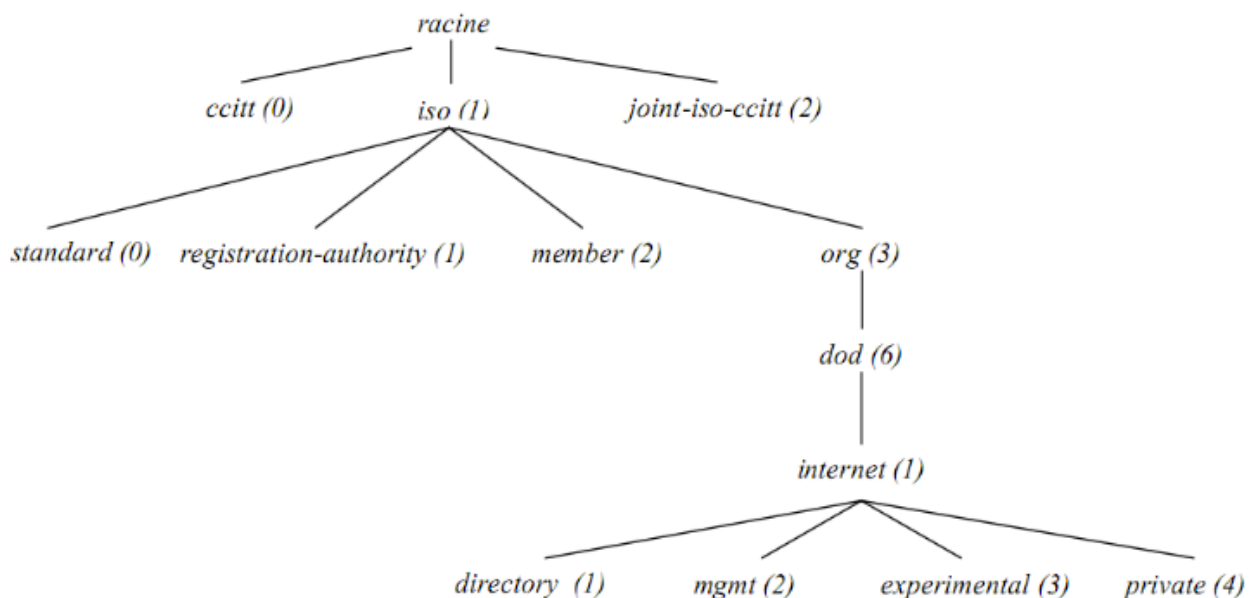
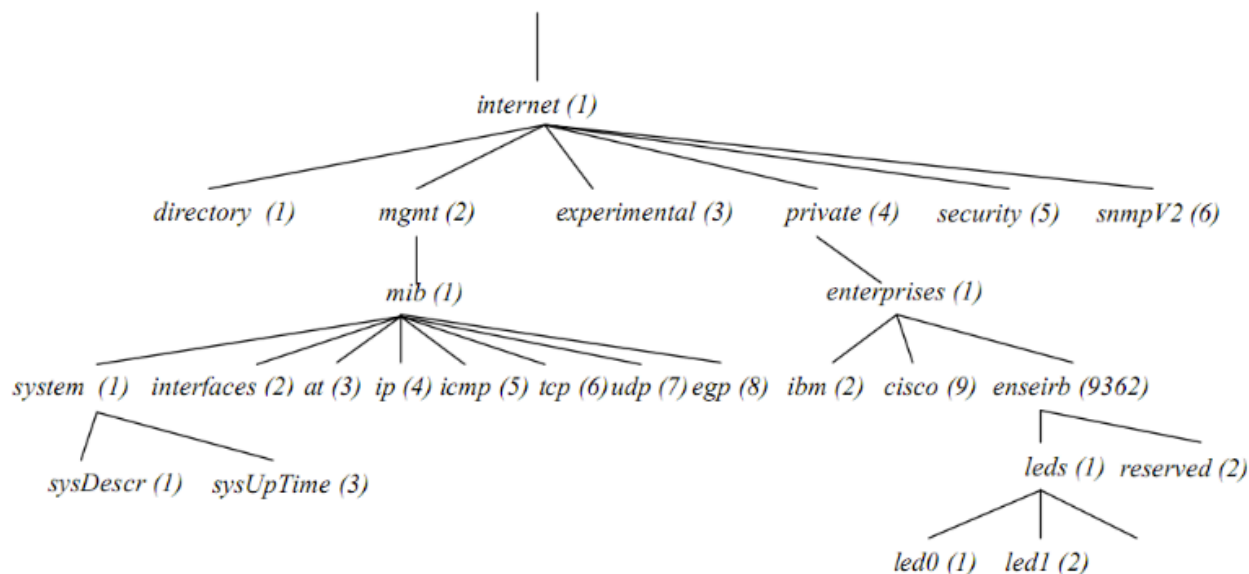


Figure 4.2: Arborescence d'une MIB standard

la branche intéressante est internet. En la détaillant on a ceci :



**Figure 4.3:** Branche internet d'une MIB

Le «0» est mis pour obtenir une feuille de la branche ainsi à ce nom symbolique, correspond l'OID suivante : 1.3.6.1.2.1.1.3.0. C'est cet OID que nous manipulerons au besoin. On peut remarquer aisément que pour tout objet intéressant, l'OID commence toujours par 1.3.6.1.2.1.

Il est à noter que si une entreprise veut définir son propre ensemble de variables de gestion, elle va enregistrer son numéro d'objet sous le noeud iso.org.dod.internet.private.entreprise.ces MIB seront dites privées et elle correspondent à la racine 1.3.6.1.4.1.

## 1.4 Nagios

D'abord lancé en 1999, Nagios a évolué pour inclure des milliers de projets développés par la communauté Nagios dans le monde entier. Nagios est officiellement parrainé par Nagios Enterprises, qui soutient la communauté que ce soit par les ventes de ses produits ou ces services commerciaux.

Le seul pré-requis pour le fonctionnement de Nagios est une machine fonctionnant sous Linux (ou une variante Unix) et un compilateur C.

Cet outil repose sur une plate-forme de supervision, fonctionnant sous Linux et sous la plupart des systèmes Unix. Il centralise les informations récoltées périodiquement par le fonctionnement modulaire dont il est caractérisé, ce qui le rend beaucoup plus attractif que ses produits concurrents. En revanche sa configuration peut se révéler complexe [14].

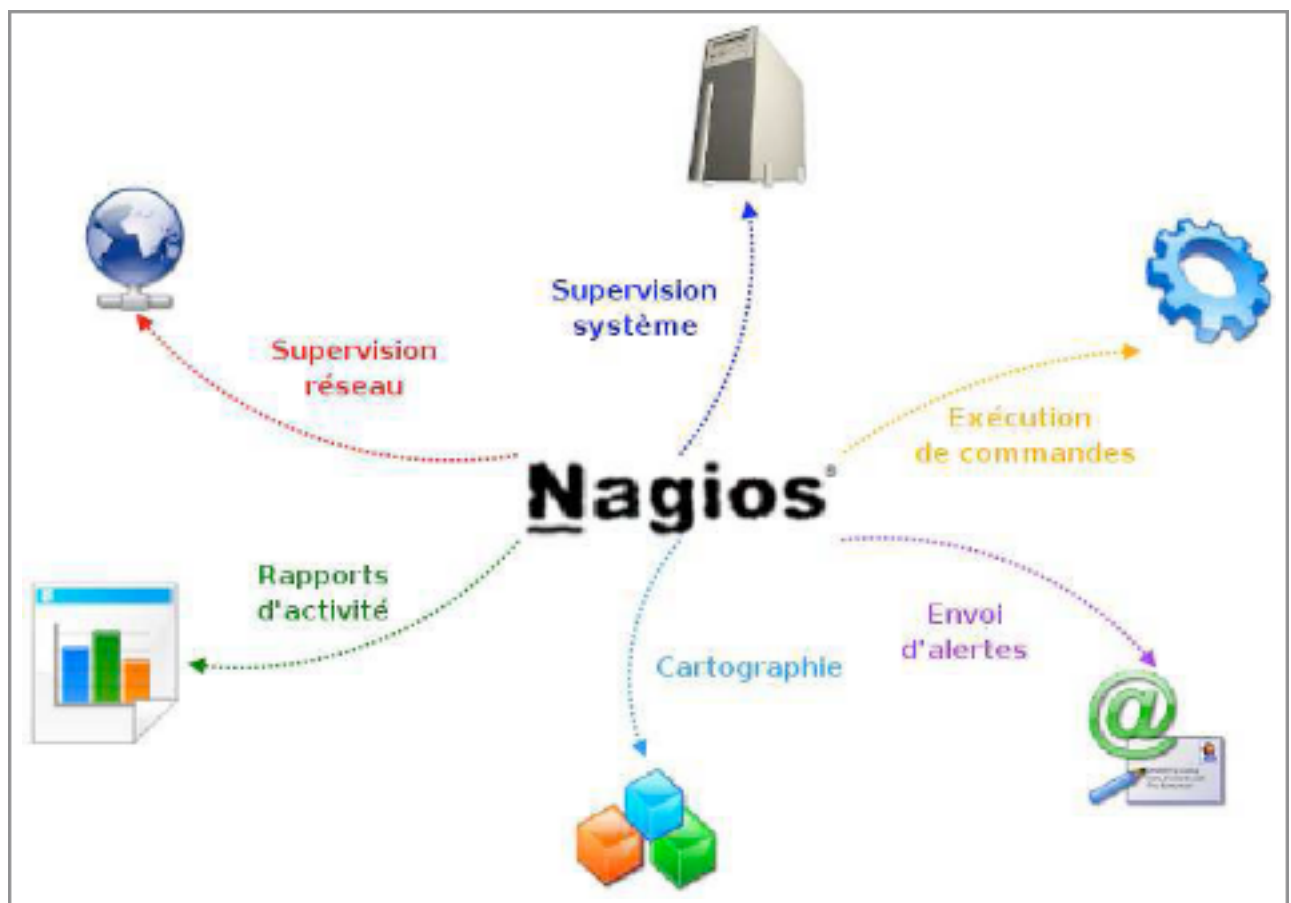
### 1.4.1 Fonctionnalités [15]

Les fonctionnalités de Nagios sont très nombreuses, parmi les plus communes nous pouvons citer les suivantes :

- supervision des différents protocoles réseaux: (SMTP, POP3, HTTP, NNTP, ICMP, SNMP, LDAP).
- supervision des ressources: (charge CPU, espace disque, mémoire utilisée, utilisateurs connectés).
- superviser des équipement réseaux: (switchs, routeur, firewall, imprimante).
- la gestion des alerte: (par email, SMS).
- génération de graphes et cartographie du réseau.
- Rotation automatiques des fichiers journaux.

Toutes ces fonctionnalités sont gérées et supervisées de manière centralisée.

La figure 2 modélise cet aspect :



**Figure 4.4:** Centralisation d'informations par Nagios

## 1.4.2 Architecture

L'architecture de Nagios repose sur le paradigme serveur-agent. Le serveur faisant office de point central de collecte des informations, tandis que les autres machines du réseau exécutent un agent chargé de renvoyer les informations au serveur.

L'architecture globale de Nagios peut être décomposée de 3 parties :

- **Un noyau:** Qui est le cœur du serveur Nagios, lancé sous forme de démon et responsable de la collecte et l'analyse des informations.
- **Des exécutants:** Ce sont les plugins (script) écrit en langage(perl,shell,c,...etc) dont un grand nombre est fourni de base, capable de fournir des informations de performance permettant à Nagios de les interpréter pour dessiner des graphes.
- **Une IHM:** Qui affiche de manière claire et concise l'état des services et des machines surveillés.

Il est possible d'ajouter à Nagios une base de données MySQL ou Postgres, lorsque le réseau à superviser est important.

La figure I. représente l'architecture de Nagios.

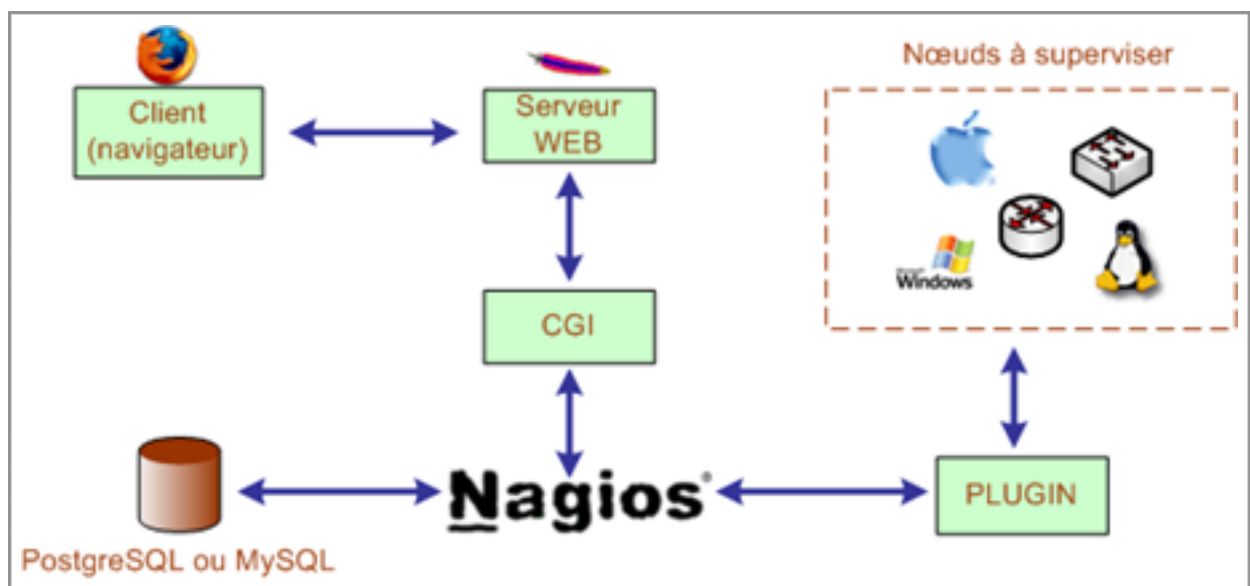


Figure 4.5: Architecture de Nagios

## 1.4.3 Plugins

Nagios fonctionne grâce à des plugins écrits en Perl ou en C. Sans ces derniers, il est totalement incapable de superviser et se résume en un simple noyau.

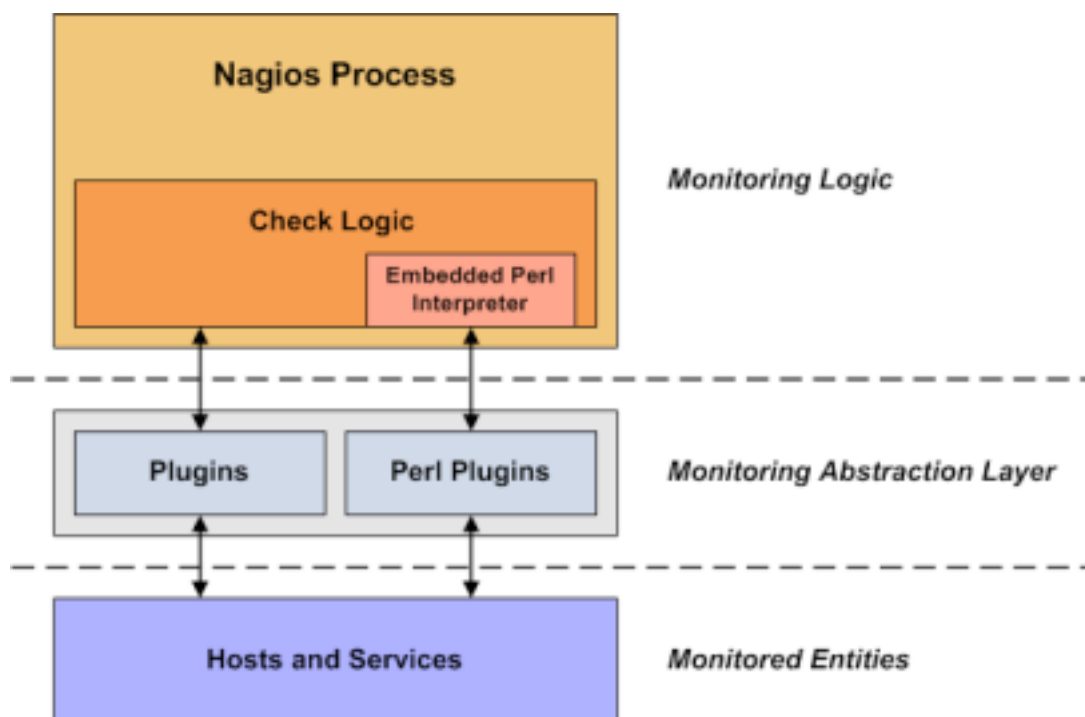
Ces plugins sont des programmes externes au serveur, des exécutables qui peuvent se lancer en ligne de commande afin de tester une station ou service. Ils fonctionnent sous le principe d'envoi de requêtes vers les hôtes ou services choisis lors d'un appel du processus de Nagios, et la transmission du code de retour au serveur principal qui par la suite traitera les résultats qu'il reçoit et prendra les mesures nécessaires.

---

Ces plugins sont capables de fournir au moteur Nagios:

- un code de retour
  - \* 0 = tout va bien (OK)
  - \* 1 = avertissement (WARNING)
  - \* 2 = alerte (CRITICAL)
  - \* 3 = inconnu (UNKNOWN)
- un court message descriptif.

Cette relation nagios et les plugins peut se résumer par la figure 4.6:



**Figure 4.6 :** Relation entre Nagios et les plugins.

Nagios possède des « packages » greffons standards regroupant les plus utilisés. Pour une utilisation basique et simple, ils devraient être suffisants. Voici quelques exemples :

- `check_http` : Vérifie la présence d'un serveur web.
- `check_load` : Vérifie la charge CPU locale.
- `check_ping` : Envoie une requête Ping à un hôte.
- `check_pop3` : Vérifie la présence d'un serveur POP3.
- `check_procs` : Compte les processus locaux.

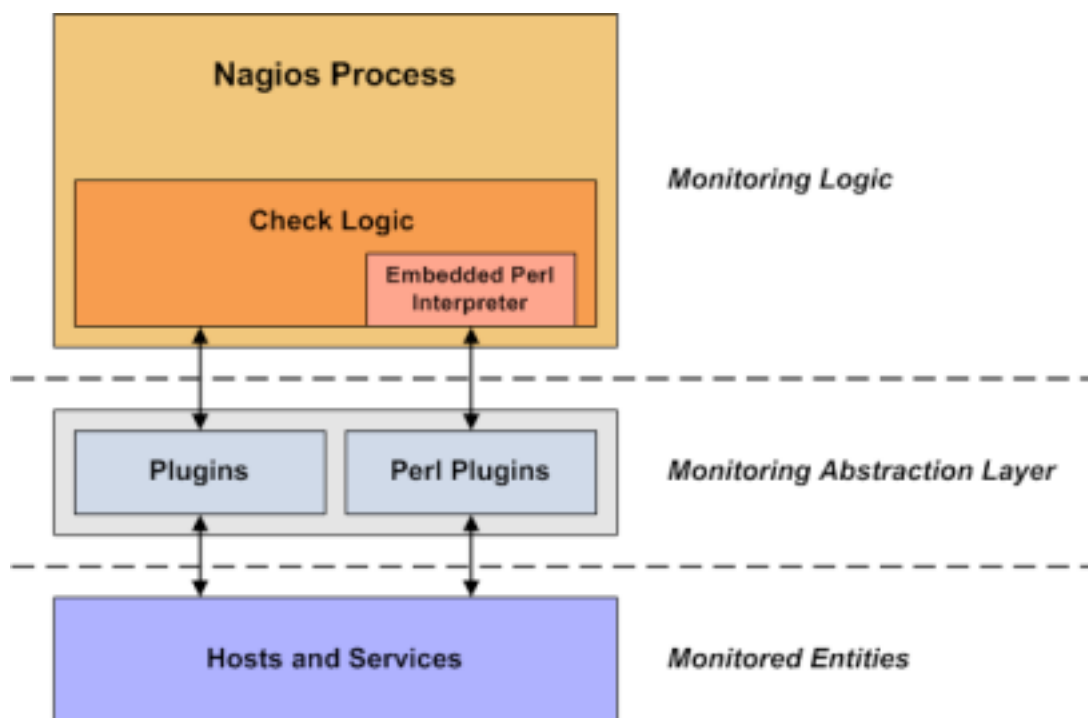
- `check_smtp` : Vérifie la présence d'un serveur SMTP.
- `check_snmp` : Envoie une requête SNMP (passée en argument) à un hôte.
- `check_ssh` : Vérifie la présence d'un service SSH.
- `check_tcp` : Vérifie l'ouverture d'un port TCP (passé en argument).
- `check_users` : Compte le nombre d'utilisateurs sur la machine locale.

Si on souhaite surveiller d'autres services ou d'autres machines, il est possible de créer son propre plugin adapté à nos besoins et l'interfacier avec Nagios tout en respectant les conventions des codes de retours précédemment expliqués. L'activité et la vivacité de la communauté Open Source et celle de Nagios 3 en particulier offre un grand nombre de plugins supplémentaires.

Les greffons peuvent fonctionner localement (directement sur la machine supervisée) ou à distance (au travers du réseau). Pour l'exécution à distance des greffons, il existe plusieurs possibilités:

- Par le biais d'autres serveurs de supervision Nagios distant. Cette méthode est utilisée dans le cadre de la supervision distribuée.
- Par les agents d'exécution de tests tels que: NRPE, NSCA, `check_by_ssh`, NSClient, etc... que nous allons définir dans le chapitre suivant.

La figure 4.7: Résume le fonctionnement des plugins.



**Figure 4.7:** Principe de fonctionnement des plugins

---

#### 1.4.4 Les fichiers de configuration [16]

Nagios s'appuie sur plusieurs fichiers textes de configuration pour construire son infrastructure de supervision. Nous allons à présent citer et définir ceux qui sont les plus importants :

- **Nagios.cfg**: Fichier de configuration de NAGIOS. A modifier par nos soins selon notre configuration et l'arborescence choisie.
- **Cgi.cfg**: Définition des paramètres des scripts CGI. Nous pouvons utiliser le fichier fourni par défaut par NAGIOS.
- **Resource.cfg**: Définition des ressources externes. Nous pouvons utiliser le fichier par défaut de NAGIOS.
- **Objects/Commands.cfg**: Définition des commandes utilisées par NAGIOS pour interroger les machines.
- **Objects/Hostclients.cfg**: Définition de toutes les machines clients à superviser (les postes utilisateurs). Ce fichier n'existe pas dans la structure de base de NAGIOS.
- **Objects/Hostservers.cfg**: Définition de toutes les machines serveurs à surveiller (serveur Web, DNS, DB,...).
- **Objects/localhost.cfg**: Il est utilisé par NAGIOS pour surveiller le serveur sur lequel est installé.
- **Objects/templates.cfg**: C'est le fichier où se trouve la définition des templates.
- **Objects/timeperiods.cfg**: Ce fichier définit les périodes de temps.
- **Objects/network.cfg**: Ce fichier est à créer, il contiendra la définition de toutes les machines composant l'infrastructure de notre réseau (routeur, switch, hub,...etc).

#### 1.5 Conclusion

À travers ce chapitre, nous avons effectué une brève présentation de la notion de supervision et de ses enjeux. Ensuite nous avons décrit l'aspect de notre solution, énuméré ses fonctionnalités et modélisé son architecture. Enfin nous avons défini les principaux fichiers de configuration de Nagios.

Dans le chapitre suivant, nous allons présenter les compléments de Nagios.

---

## Chapitre 2 : Les compléments de Nagios

Dans ce chapitre nous allons présenter tout outils ou compléments que nous ajouterons à Nagios afin de mettre en valeur les fonctionnalités qu'il offre, optimiser, enrichir et garantir la mise en place d'une solution complète, facile à administrer et qui répond aux besoins que nous nous sommes fixés.

### 2.1 NDOutils

NDOutils nous permet d'exporter les données actuelles et historiques à partir d'une ou plusieurs instances de Nagios vers une base de données MySQL plutôt que de ne les garder que dans les fichiers plats. De cette façon, les données seront plus souples à gérer. Son interaction avec Nagios est indépendante de Centreon [17].

#### 2.1.1 Utilités

- Stockage des données à long terme.
- Permettre à un logiciel tiers comme « Centreon » d'accéder de manière optimisée aux données d'états et de performances de Nagios et de partager ses données.
- Optimisation de l'exploitation des données et amélioration des performances; il est plus rapide de rechercher des informations dans une base de données structurée, plutôt que dans un fichier de journalisation qu'il faut parcourir entièrement à chaque utilisation.

#### 2.1.2 Architecture

NDOutils se compose d'un démon autonome et d'un courtier d'événement Nagios :

- **Ndo2db**: Démon nécessitant un script d'initialisation et responsable de l'ouverture de socket (Unix ou TCP) et place les données trouvées dans une base de données MySQL.
- **Ndomod**: Lancé automatiquement avec Nagios et responsable de l'exportation des données extraites des fichiers plats pour les déposer dans un socket (Unix, TCP).

Nous pouvons avoir plusieurs serveurs Nagios comme le montre la figure ci dessous:



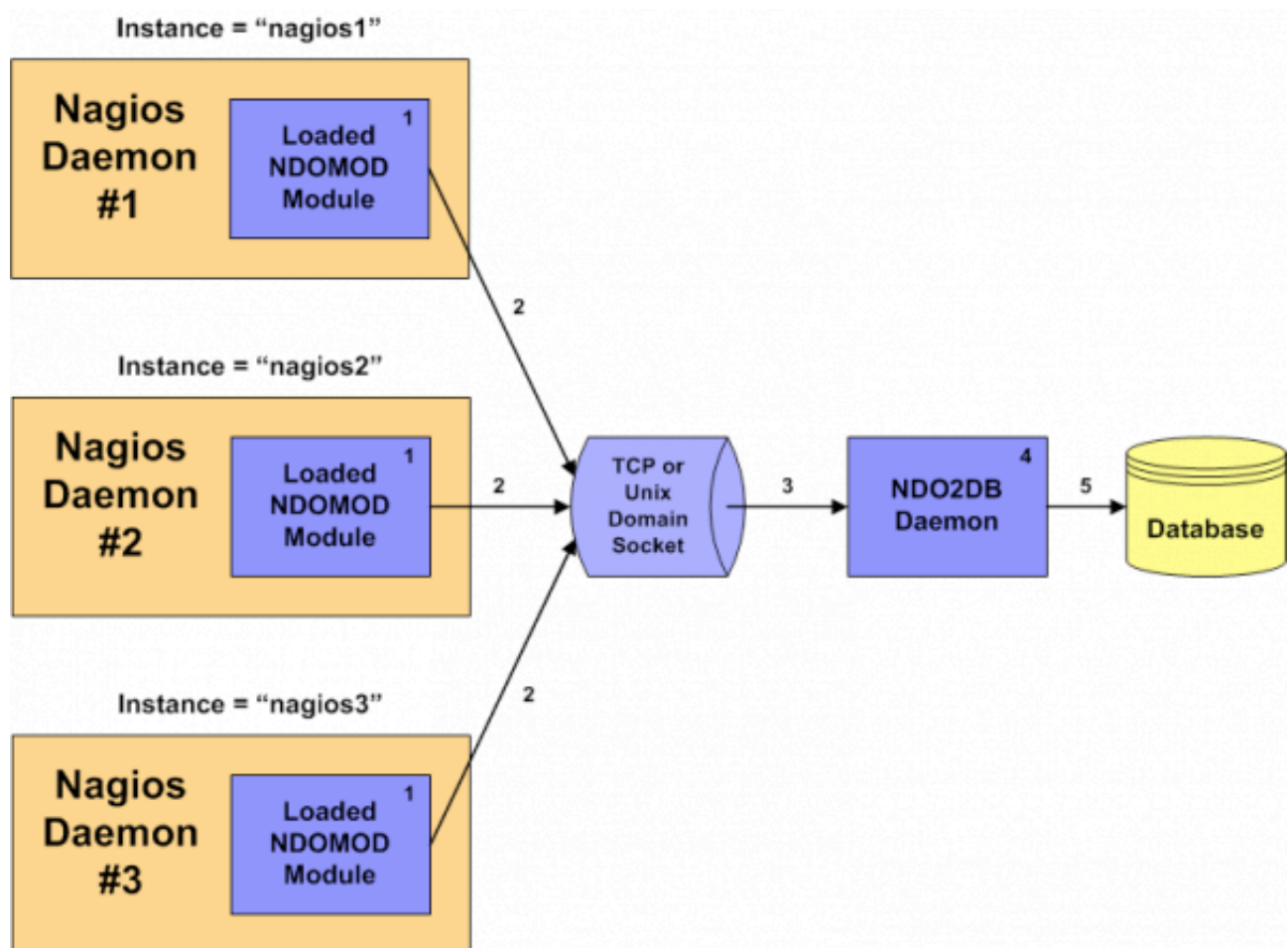


Figure 5.1: Architecture NDOutils.

## 2.2 Centreon

Centreon est le dérivé français de Nagios de référence développé par la société Merethis. Il s'agit d'une couche applicative Web venant se greffer à Nagios pour offrir une administration moins rudimentaire (évite les fichiers de configuration et les lignes de commandes brutes). L'équipe de Merethis est avant-gardiste et a inspiré pour certains points les lignes directrices de la communauté. C'est un produit complet et son interface le rend très professionnel aux yeux des dirigeants. Basée sur deux fonctionnalités principales[19] :

- **Une seconde interface de monitoring:** Centreon propose une interface plus intuitive et sobre.
- **Puissante interface de configuration:** Désormais, nous pouvons modifier la configuration de Nagios depuis le navigateur web sans avoir à manipuler les fichiers éparpillés sur le disque.

Centreon possède sa propre version de chaque fichier de configuration de Nagios. Lorsque l'utilisateur modifie un paramètre par l'interface Centreon, ce changement est d'abord répercuté sur les fichiers "de copies" de Centreon. Pour que les modifications soient prises en compte par Nagios, il faut exporter les fichiers stockés dans l'arborescence de Centreon et recharger Nagios.

---

## 2.2.1 Utilités

La modification manuelle de ces fichiers de configuration, à chaque ajout une hôte, un service, une commande augmentera le risque de générer beaucoup plus d'erreur.

On a donc choisi de coupler Nagios à Centreon pour remédier à ce problème en évitant la modification à la main de ces fichiers textes. Il dispose également d'une interface multi-utilisateurs, intuitive et personnalisable avec intégration des droits d'accès en plus d'un compte rendu graphique plus pratique et élégant que celui offert par Nagios.

## 2.2.2 Architecture

### 2.2.2.1 Centreon et Base de données [20]

Centreon interagit principalement avec la base de données MySQL pour remonter les données extraites par Nagios et stockées dans la base de données grâce à NDO.

Lors de son installation Centreon crée automatiquement trois schémas dans la base de données MySQL :

- **Centstatus:** C'est la base de données dans laquelle NDOUtils stocke les données extraites des fichiers plats de Nagios et sur laquelle Centreon pointe pour pouvoir remonter les mêmes données.

Ces données sont visualisées dans l'interface monitoring de Centreon.

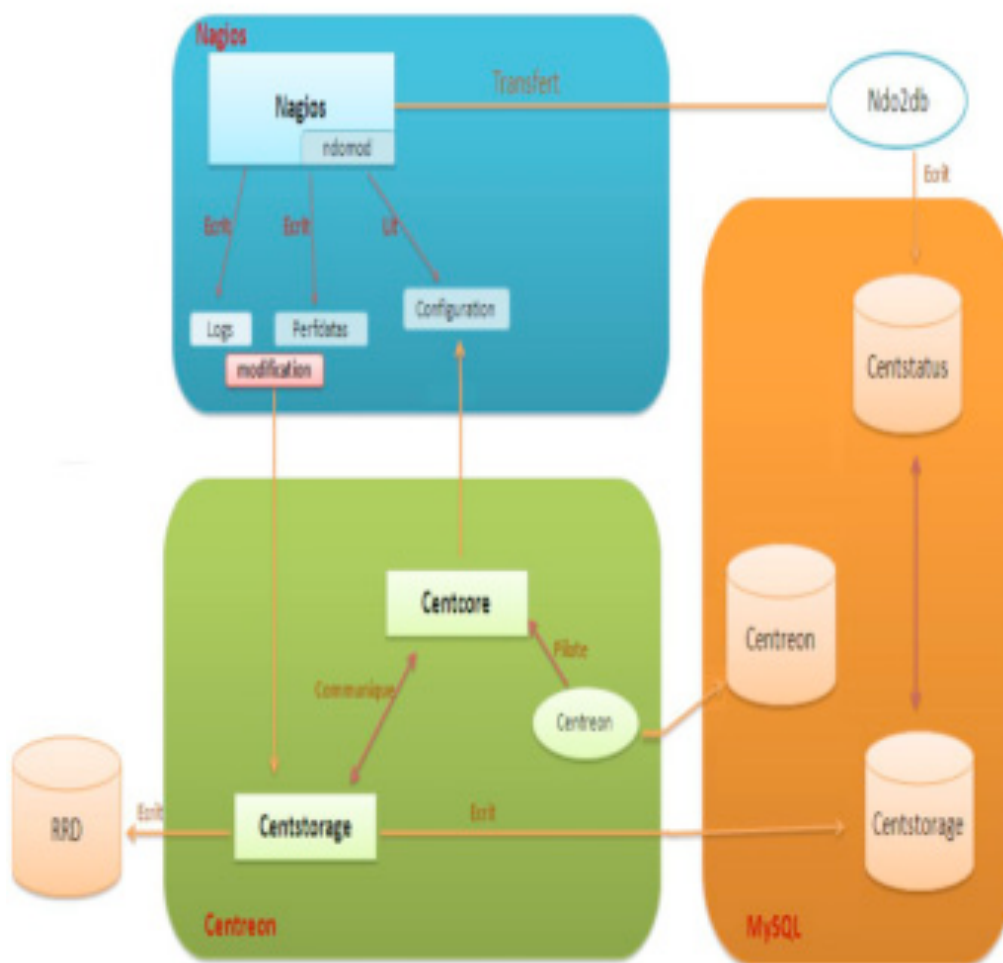
- **Centstorage:** Centstorage est l'outil qui exploite les données remontées par Nagios pour Centreon. C'est un programme écrit en Perl, associé à Centreon. À chaque modification du fichier de données perfddata, centstorage met à jour deux bases de données. Tout d'abord, afin de stocker les données sur le long terme, Centstorage utilise une base de données MySQL. Par ailleurs, à chaque exécution, Centstorage met à jour des « Round Robin Databases » notées RRD.
- **Centreon:** Collecte les informations de configuration et stocke les fichiers objets de Nagios (Host, Services, Périodes, ....etc). Grâce aux fonctions d'Import/Export, Centreon peut générer de nouveaux fichiers de configuration pour Nagios.

### 2.2.2.2 Centreon et démons [20]

Pour un fonctionnement sain, Centreon a besoin que ses deux démons soient lancés :

- **Centstorage :** Centstorage est l'outil qui exploite les données remontées par Nagios pour Centreon. C'est un programme écrit en Perl, associé à Centreon. À chaque modification du fichier de données perfddata, centstorage met à jour deux bases de données «Centstorage» et «RRD».
- **Centcore :** Dans le cas d'une architecture distribuée (serveur centrale pour la supervision et d'autres serveurs fils), est chargé d'exporter la configuration des moteurs de supervision vers le serveur central et satellites ainsi que du redémarrage des moteurs de supervision vers Nagios.

La figure 5.2 est un schéma récapitulatif décrivant l'interaction entre les différentes couches logicielles de l'association entre Nagios et Centreon.



**Figure 5.2:** Interaction entre Nagios et Centreon.

### • Explication des interactions entre Nagios et Centreon [18]:

Centreon dispose de sa propre base de données qui stocke les informations qu'on renseigne dans l'interface (nouvel hôte, nouveau groupe, nouvelles commandes, nouveaux services, ...etc).

Après chaque modification, il faut exporter la configuration. Cela a pour effet d'écraser les fichiers de configuration de Nagios (dans /etc/nagios) avec les dernières modifications réalisées sur l'interface Centreon.

NDOUtils est un module officiel de Nagios qui est à l'écoute des événements de Nagios. C'est NDOMOD qui intercepte ces mises à jour afin de pouvoir les stocker dans la base de données. Directement après l'export sur l'interface Centreon de la configuration Nagios (et du redémarrage de Nagios), NDOUtils intercepte ces informations et met à jour la base de données nommée ndo.

Cette base de données contient toutes les informations des hôtes, de leurs status ... Elle est constamment mise à jour.

Les informations que Centreon affiche dans la page d'accueil, dans l'onglet supervision sont issues de la base de données ndo et sont exactement les mêmes que celles affichées sur l'interface Nagios.

Centreon sert donc à la visualisation des informations, à la génération de la configuration Nagios avec une véritable interface complète, à la possibilité d'extraire des informations à l'aide de rapports. Nagios réalise le travail d'investigation sur les serveurs, éléments réseaux..., les données qu'il récupère sont exploitable par Centreon à travers ses rapports grâce au travail de NDOUtils.

## 2.3 NSClient pour la supervision des serveurs Windows

C'est un plugin permettant de récupérer un nombre important d'informations à surveiller sur une machine Windows. Le plugin se livre avec un ensemble de commandes check qui nous permettent de dégager d'importantes informations comme [17]:

- **CLIENTVERSION** : retourne la version de l'agent NSClient.
- **CPULOAD** : Retourne la charge moyenne du système.
- **UPTIME** : Retourne la durée écoulée depuis le dernier redémarrage de la machine.
- **USEDISKSPACE** : Retourne la taille et le pourcentage du disque utilisé.
- **MEMUSE** : Retourne la taille de la mémoire utilisée et la taille restante.
- **SERVICESTATE** : Retourne le statut (démarré, arrêté) d'un ou plusieurs services Windows.
- **PROCSTATES** : Vérifie si un ou plusieurs processus sont démarrés.
- **COUNTER** : Interroge n'importe quel compteur de performance.

### 2.3.1 Architecture

NSClient se base sur une architecture client/serveur (Figure II.3). La partie cliente nommée check\_nt, doit être disponible sur le serveur Nagios et on doit vérifier son existence parmi les plugins délivrés avec Nagios-plugins sinon l'installer. La partie serveur NSClient++ est à installer sur chacune des machines Windows à surveiller.

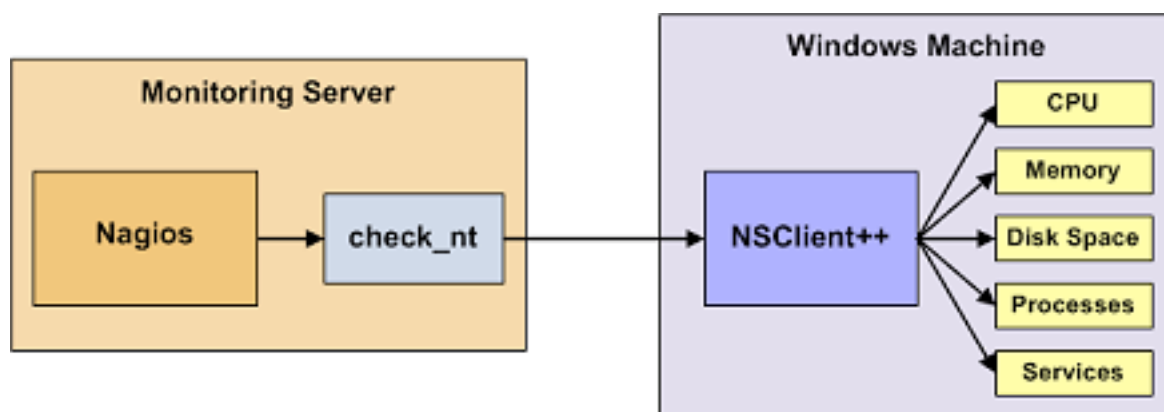


Figure 5.3: Architecture NSClient

## 2.4 NRPE pour la supervision des serveurs Linux

NRPE (Nagios Remote Plugin Executor) est un agent de supervision qui permet de récupérer les informations à distance lors de la supervision d'un serveur Linux. Son avantage principale est qu'il permet de réduire les charges sur le serveur nagios en exécutant les commandes directement sur la machine à superviser. Il est livré avec un pack de commandes check définis par défaut dans son fichier de configuration et nécessite l'installation des plugins Nagios aussi [17].

### 2.4.1 Architecture

NRPE se base sur une architecture client/serveur (Figure 2.4). La partie cliente nommée `check_nrpe`, doit être disponible sur le serveur Nagios et on doit vérifier son existence parmi les plugins délivrés avec Nagios-plugins sinon l'installer. La partie serveur NRPE est à installer sur chacune des machines Windows à surveiller.

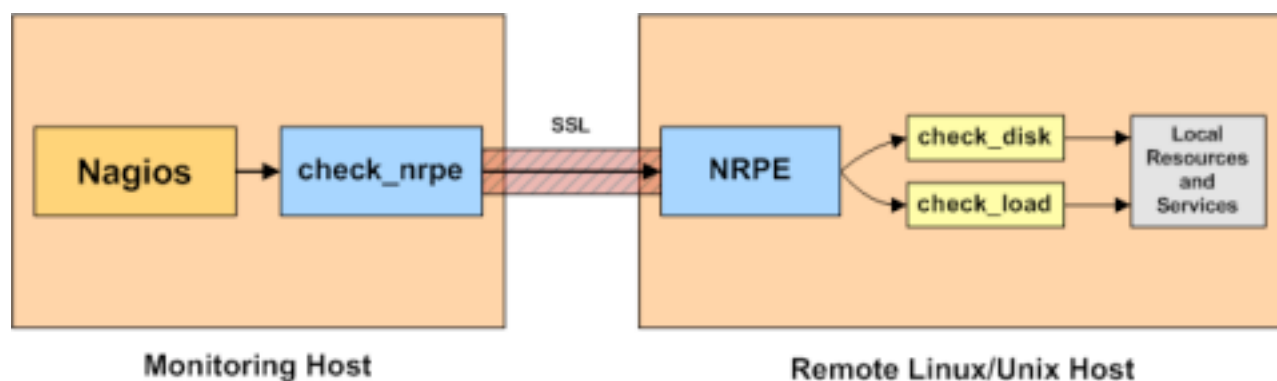


Figure 5.4: Mécanisme du NRPE

#### Procédure de fonctionnement :

- Le serveur Nagios demande l'exécution d'un plugin sur la machine distante.
- Le daemon NRPE hébergé sur la machine distante, reçoit la requête d'exécution du plugin.
- Le plugin est exécuté sur la machine distante.
- Le daemon NRPE de la machine distante envoie le résultat du plugin au serveur Nagios.
- Le serveur Nagios interprète les résultats reçus.

### 2.5 Conclusion

Le but de ce chapitre était de présenter les compléments que nous avons choisis à Nagios. Certains ont été choisis pour leur nécessité comme les greffons NRPE et NSClient, et d'autres participaient surtout à l'amélioration de la manipulation et l'utilisation de Nagios et également facilité sa configuration. Dans le chapitre suivant, nous entamerons les différentes étapes de configuration et montrer quelques exemple d'utilisation.

---

## Chapitre 3: Mise en place du système de supervision

Au sein de ce dernier chapitre, nous allons présenter l'environnement de travail et enfin quelques captures écrans des interfaces de Nagios/Centreon.

### 3.1 Environnements de mise en place

#### 3.1.1 Environnement matériel

- Phase de test : Au cours de cette phase, on a installé une machine virtuelle sur notre machine personnelle pour tester la solution choisie et s'adapter à sa mise en place, mais aussi de s'assurer si elle répond vraiment aux besoins fixés par la société avant de passer à la phase de production et ce en essayant de tester deux serveurs distants Windows et Linux.
- Phase de production : Une douzaine de serveurs Windows et Linux à superviser. Nous avons installés un serveur Linux (hardware et système exploitation) pour y déployer Nagios/Centreon qui a les caractéristiques suivantes ;
  - Système Debian-7.8.0-amd64 (i386).
    - Microprocesseur Intel® Core ®2 Duo de vitesse 2.66GHz.
    - Connexion internet.

#### 3.1.2 Environnement logiciel

- La solution de supervision Nagios-3.5.1
- Les greffons de Nagios, Nagios-plugins-2.0.3
- La couche applicative associée à Nagios pour faciliter sa configuration et son administration
- Centreon-2.6.0
- Le plugin NDOutils-1.5.2 pour le stockage des données de Nagios dans la base de données MySQL et le partage de ces données avec Centreon.
- Le plugin NSClient pour la supervision des serveurs Windows.
- Le plugin NRPE-2.15 pour la supervision des serveurs Linux.

### 3.1.3 Topologie réseau liée à la supervision de l'EPB

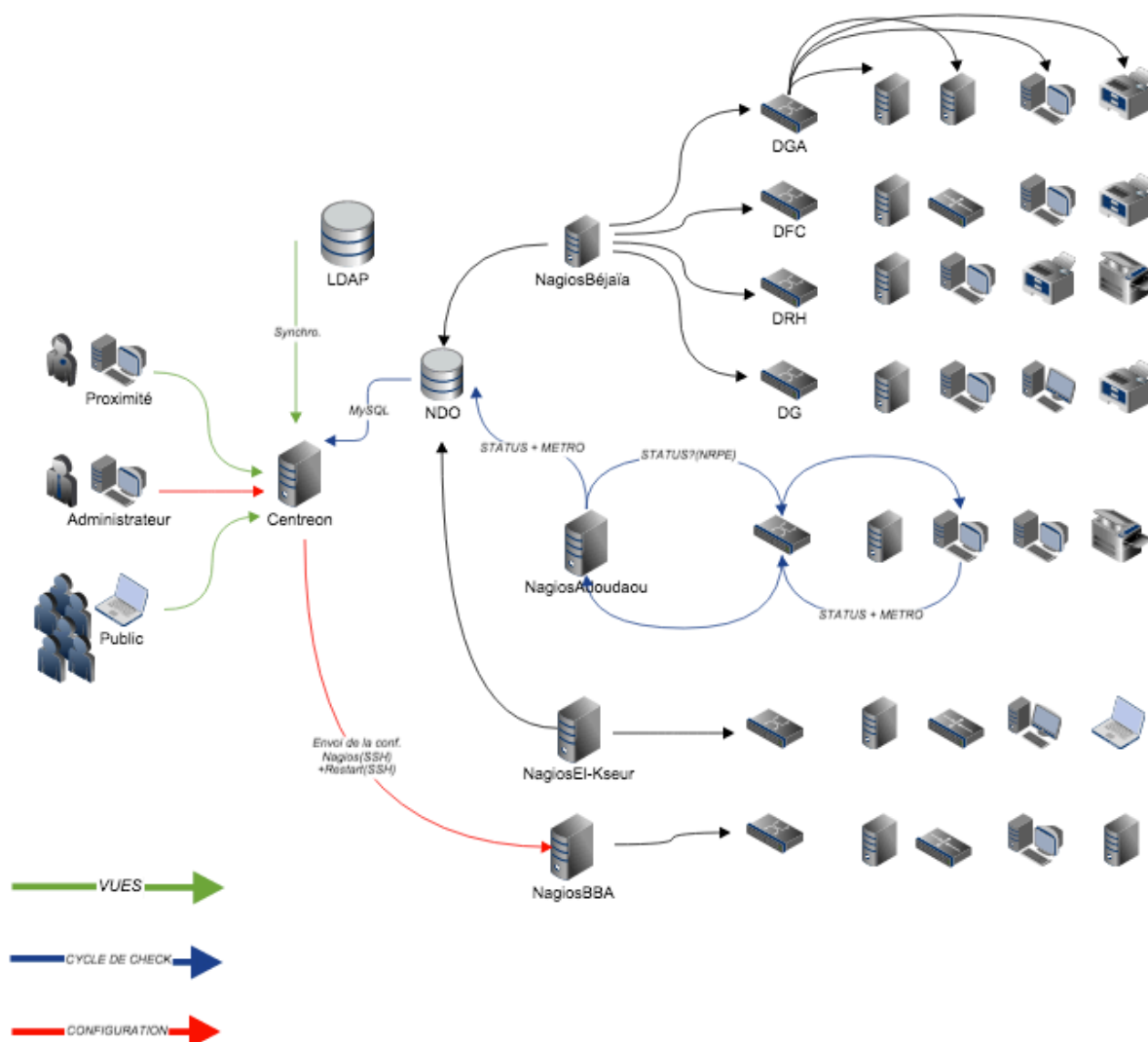


Figure 6.1: Schéma de la topologie réseau liée à la supervision de l'EPB.

## 3.2. Mise en place de Nagios/Centreon et les plugins [22]

### 3.2.1 Pré-requis Nagios/Centreon

En plus des plugins Nagios, nous devons installer certaines dépendances nécessaires au bon fonctionnement de Nagios. Les pré-requis à l'installation sont :

- Dépendances LAMP : Apache2, PHP5, MySQL.
- Librairie Perl: libperl-dev.
- Serveur SNMP: SNMP, SNMPPD .
- Les bibliothèques graphiques : GD, libgd libpng, libjpeg, libgd2-xpm-dev...

- Compilateur : gcc, gcc-gc++ .
- Serveur de messagerie: postfix.
- Paquets divers: dsb-mailx, lsb-release...

### 3.2.2 Installation de Nagios/Centreon

Les étapes d'installation et de configuration de « Nagios-3.5.1 » et ses plugins « Nagios-plugins-2.0.3 », « Centreon-2.6.0 » et « NDOUtils-1.5.2 » seront détaillées dans l'annexe A.

### 3.2.3 Installation de NSClient

Pour la supervision des serveurs Windows, nous devons installer le greffon NSClient sur la machine distante et vérifions la présence de la commande « check\_nt » parmi les plugins installés de Nagios. Les étapes d'installation seront détaillées dans l'annexe B.

### 3.2.4 Installation de NRPE

Pour la supervision des serveurs Linux, nous allons installer le greffon « NRPE-2.15 » sur la machine distante et vérifions la présence de la commande « check\_nt » parmi les plugins installés de Nagios. Les étapes d'installation seront détaillées dans l'annexe C.

## 3.3 Interfaces de Centreon [21]

- Tactical Overview

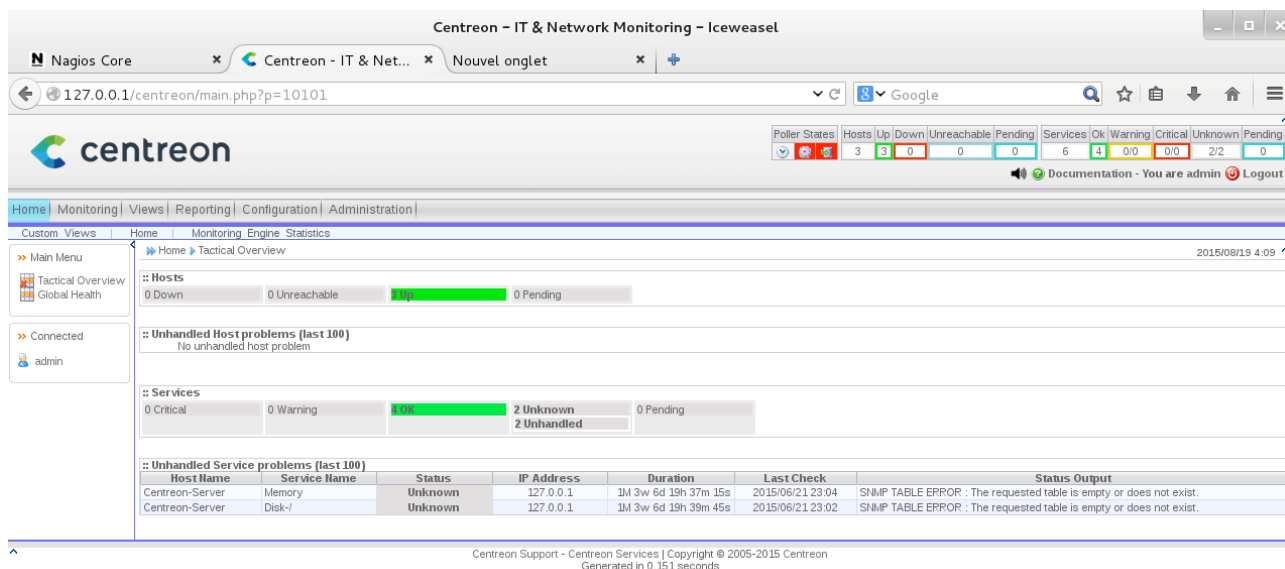


Figure 6.2: Interface de vue globale.



## • Statistique de Nagios

Cette vue, nous offre la possibilité de visualiser les performances de notre supervision (temps de check, latence etc..) et des graphiques traçant l'historique de performances de chacune de nos instances.

## • Temps de check, latence

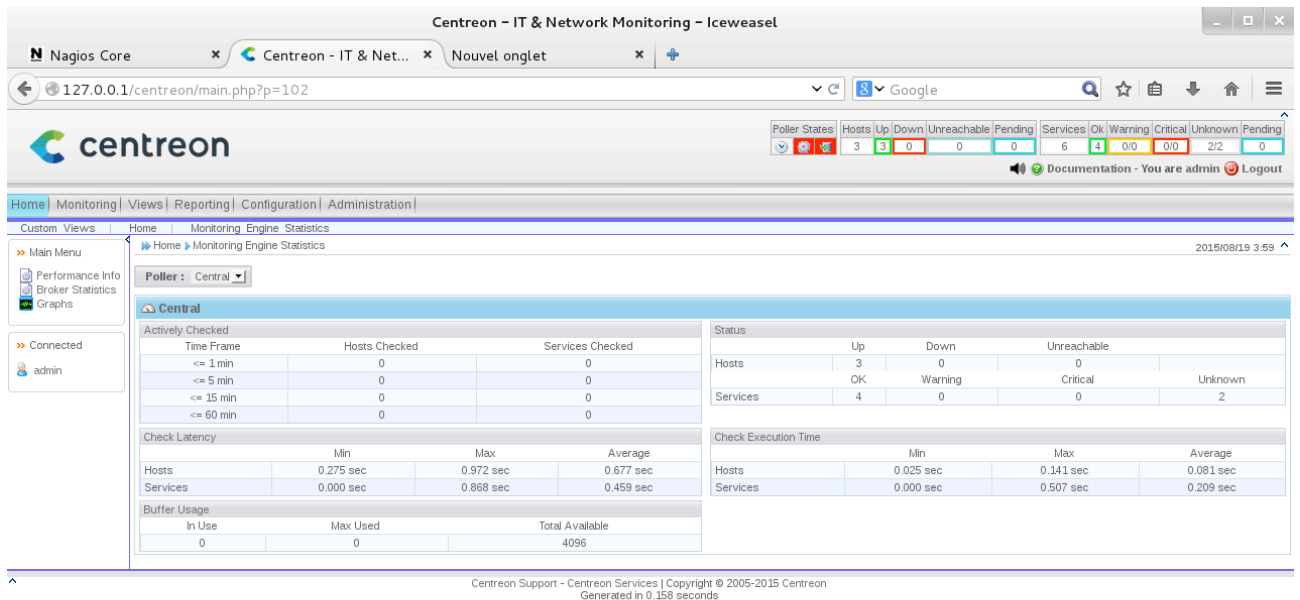


Figure 6.3: Interface des statistiques Nagios.

## • Graphique de performance



Figure 6.4: Interface de graphiques de performance.

# • Monitoring

## • Les hôtes

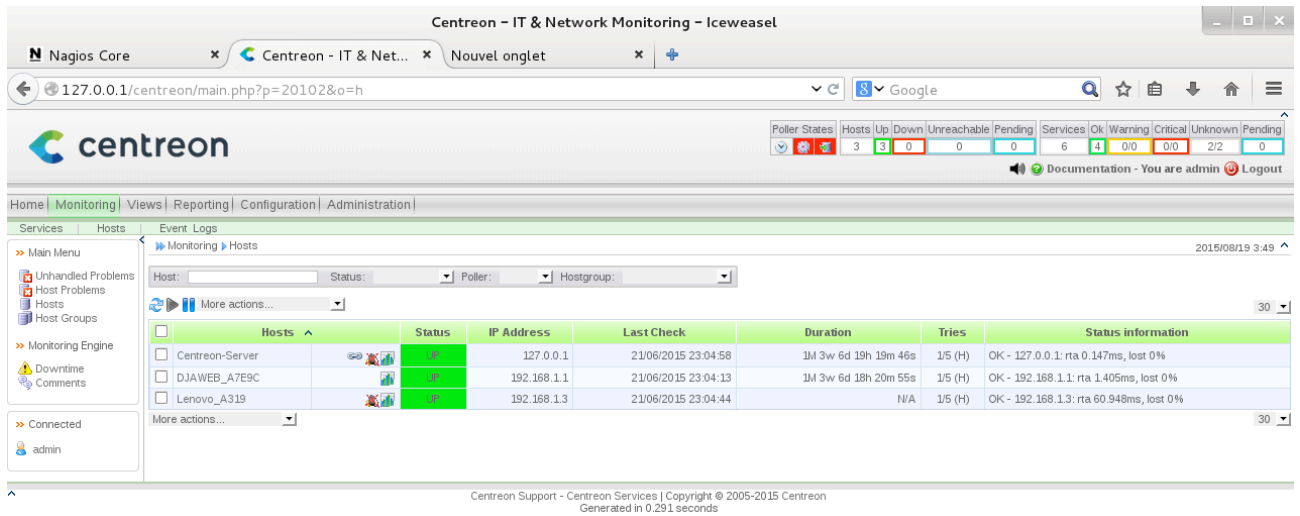


Figure 6.5: Interface des hôtes supervisés.

## • Les services

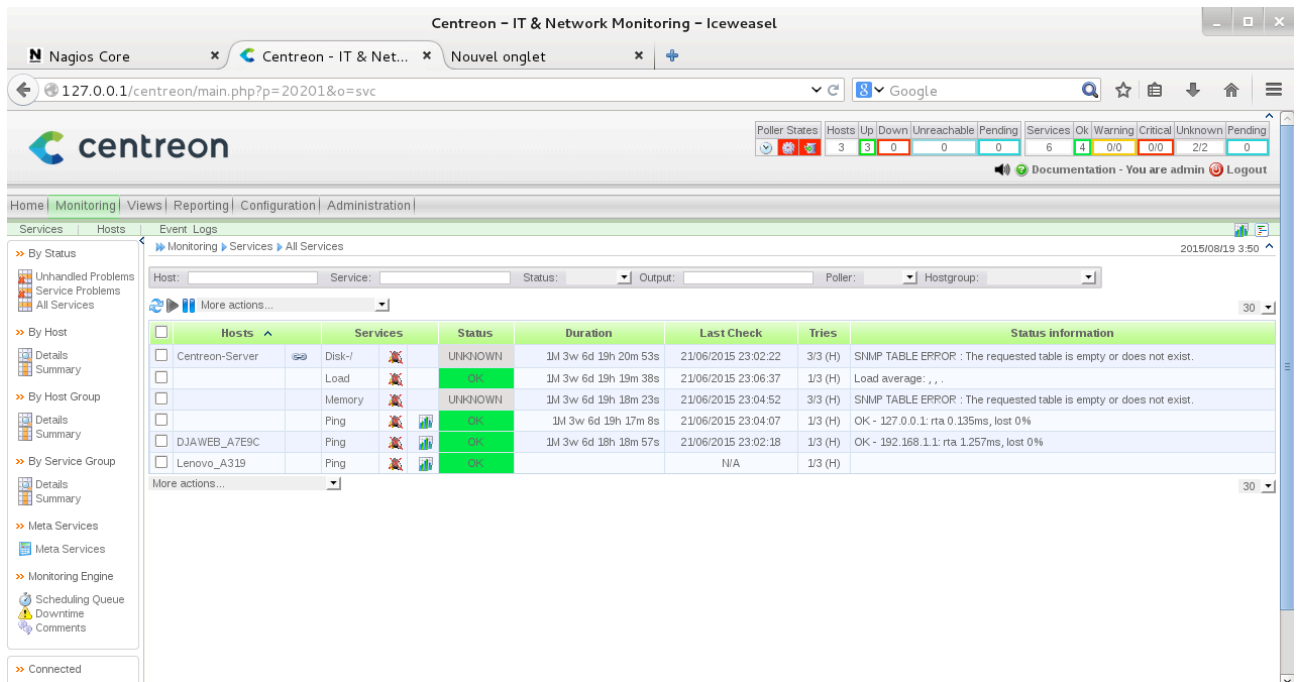


Figure 6.6: Interface des services supervisés.

## • Event logs

Cette vue, nous donne l'accès à tout l'historique des journaux d'évènements concernant Centreon (Nagios).

Day	Time	Object name	Status	Type	Retry	Output	Contact	Command
2015/06/21	23:04:44	DJAWEB_A7E9C	OK	HARD	1	INITIAL STATE		
2015/06/21	23:04:38	DJAWEB_A7E9C	OK	HARD	1	OK - 192.168.1.1: rta 1.405ms, lost 0%		
2015/06/21	22:59:13	DJAWEB_A7E9C	OK	SOFT	3	OK - 192.168.1.1: rta 1.063ms, lost 0%		
2015/06/21	22:58:08	DJAWEB_A7E9C	CRITICAL	SOFT	2	CRITICAL - 192.168.1.1: rta nan, lost 100%		
2015/06/21	22:57:03	DJAWEB_A7E9C	CRITICAL	SOFT	1	CRITICAL - 192.168.1.1: rta nan, lost 100%		
2015/06/21	22:51:58	DJAWEB_A7E9C	OK	HARD	1	OK - 192.168.1.1: rta 1.534ms, lost 0%		
2015/06/21	22:46:53	DJAWEB_A7E9C	OK	HARD	1	OK - 192.168.1.1: rta 1.857ms, lost 0%		
2015/06/21	22:45:38	DJAWEB_A7E9C	OK	HARD	1	INITIAL STATE		
2015/06/21	22:41:48	DJAWEB_A7E9C	OK	HARD	1	OK - 192.168.1.1: rta 0.968ms, lost 0%		
2015/06/21	22:36:48	DJAWEB_A7E9C	OK	HARD	1	INITIAL STATE		
2015/06/21	22:36:45	DJAWEB_A7E9C	OK	HARD	1	OK - 192.168.1.1: rta 1.191ms, lost 0%		
2015/06/21	22:33:05	DJAWEB_A7E9C	OK	HARD	1	INITIAL STATE		
2015/06/21	22:31:42	DJAWEB_A7E9C	OK	HARD	1	OK - 192.168.1.1: rta 1.092ms, lost 0%		
2015/06/21	22:26:37	DJAWEB_A7E9C	OK	HARD	1	OK - 192.168.1.1: rta 6.332ms, lost 0%		
2015/06/21	22:25:42	DJAWEB_A7E9C	OK	HARD	1	INITIAL STATE		
2015/06/21	22:21:35	DJAWEB_A7E9C	OK	HARD	1	OK - 192.168.1.1: rta 1.438ms, lost 0%		
2015/06/21	22:16:30	DJAWEB_A7E9C	OK	HARD	1	OK - 192.168.1.1: rta 1.263ms, lost 0%		
2015/06/21	22:11:25	DJAWEB_A7E9C	OK	HARD	1	OK - 192.168.1.1: rta 2.436ms, lost 0%		

Figure 6.7: Interface des journaux d'évènements.

### 3.4 Notification par mail

En plus d'être informé visuellement par l'interface de Centreon ou Nagios, on peut configurer l'envoi des emails pour nous informer la perte d'un hôte ou d'un service. Cela permet d'avoir des informations supplémentaires et d'avoir un historique de l'activité durant l'absence de l'administrateur.

Pour mettre en place ce dispositif, on aura besoin d'installer les éléments postfix et mailx et avoir accès à un serveur SMTP (propre à la société). Voir [Annexe C]

Centreon possède déjà les commandes de notifications « host-notify-by-email » et « service-notify-by-email » dans la partie configuration > commands > notifications qui seront paramétrées à des hôtes ou services lors de leur création, ainsi on gardera la même configuration à chaque nouvel ajout.

Il nous reste qu'à informer le système des utilisateurs et groupes d'utilisateurs à notifier lors de l'apparition d'un problème et de sélectionner la durée de notification.

Cette configuration est claire dans la figure 3.8 .

The screenshot shows the 'Modify an Escalation' configuration page in Nagios. The breadcrumb navigation is 'Configuration > Notifications > Escalations'. The page title is 'Modify an Escalation' and the current time is '2015/09/07 4:11'. There are tabs for 'Information', 'Hosts Escalation', 'Services Escalation', 'Hostgroups Escalation', 'Meta Services Escalation', and 'Servicegroups Escalation'. The 'Information' tab is active. The form contains the following fields and options:

- Escalation Name: Lenovo\_A319
- Alias: (empty)
- First Notification: 3
- Last Notification: 0
- Notification Interval: 0 \* 60 seconds
- Escalation Period: 24x7
- Hosts Escalation Options:  Down,  Unreachable,  Recovery
- Services Escalation Options:  Warning,  Unknown,  Critical,  Recovery
- Linked Contact Groups: A list of 'Available' groups (Guest) and a list of 'Selected' groups (Supervisors). There are 'Add' and 'Remove' buttons between the lists.
- Comments: (empty text area)

At the bottom, there are radio buttons for 'List' (selected) and 'Form', and 'Save' and 'Reset' buttons.

**Figure 6.8:** Configuration des notifications.

Cette interface modélise la configuration d'envoi de notification, où nous devons sélectionner les utilisateurs concernés par la réception de ces notifications, ainsi on définira l'intervalle de notification, la période de notification (24\*7, workhours,...) et le type de notifications.

### 3.5 Conclusion

Dans ce chapitre, nous nous sommes focalisés sur l'aspect pratique de notre projet, tout en détaillant les étapes de mise en place et l'utilité de notre solution. L'apport important de Centreon à Nagios est principalement, la facilité de la configuration, mais aussi la possibilité d'obtenir des rapports et d'analyses plus rapide et d'une manière plus précise dans but de prévenir avant que les pannes paralyse le système et ainsi gagner et optimiser la gestion de son temps.

---

## Conclusion générale

Le travail que nous avons accompli a pour principal objectif la proposition de deux solutions pour le port de Béjaïa : La première étant une architecture VPN basée sur la technologie MPLS, la deuxième solution est la mise en place d'un système de supervision pour les quatre pôles de l'EPB. Ce projet nous a permis de mettre en pratique les connaissances acquises durant le cycle de notre formation et de nous familiariser avec le monde professionnel durant la période de notre stage au sein de l'entreprise d'accueil.

Dans ce mémoire, nous avons présenté dans la première partie quelques généralités sur les VPNs, les différents protocoles utilisés et le principe de fonctionnement des réseaux MPLS. Enfin nous avons configuré l'architecture proposée à l'aide de l'outil GNS3 afin de simuler l'interconnexion des différentes plate-formes. En effet, la combinaison entre les technologies VPN et MPLS a permis de fournir une solution sécuritaire.

Dans la deuxième partie, nous avons expliqué les concepts de la supervision et son principe de fonctionnement dans un système d'information. Ensuite, nous avons mis en évidence l'architecture proposée. Le choix de l'association de Centreon à Nagios n'étant plus à démontrer, ces deux logiciels compatibles et matures étant très utilisés dans le monde professionnel font d'eux des outils incontournables dans le monde de la supervision mais aussi le propos de ce projet était de choisir une solution qui répondait aux besoins organisationnels et financiers de l'entreprise.

Entre autres, l'évolution dans le domaine des réseaux et de la supervision ne cesse de donner une grande souplesse pour trouver des solutions efficaces pour certains dangers et pour fournir une sécurité des biens et des personnes.

La réalisation de ce projet a été bénéfique et fructueuse pour nous dans le sens où elle nous a permis d'apporter une contribution au port de Béjaïa, mais aussi d'approfondir et d'acquérir de nouvelles connaissances qui seront utiles et déterministes pour nous à l'avenir.

---

## Annexe A

### I. Installation de Nagios

#### I.1 Installation des bibliothèques et pré-requis nécessaires :

Nous installerons ici, les outils, logiciels ainsi que les dépendances dont Nagios a besoin pour bien fonctionner. La méthode ici est l'utilisation de l'invite de commande. Pour installer un paquet de nom paquet(X), nous utiliserons la commande :

```
prompt > apt-get install paquet(X).
```

Pour ce faire, nous préparerons notre système en y installant plusieurs logiciels et bibliothèques :

- Le compilateur : **apt-get install build-essential ;**
- Le serveur web et PHP5: **apt-get install apache2 php5;**
- serveur SNMP : **apt-get install snmp snmpd ;**
- **Paramétrage du serveur SNMP:**

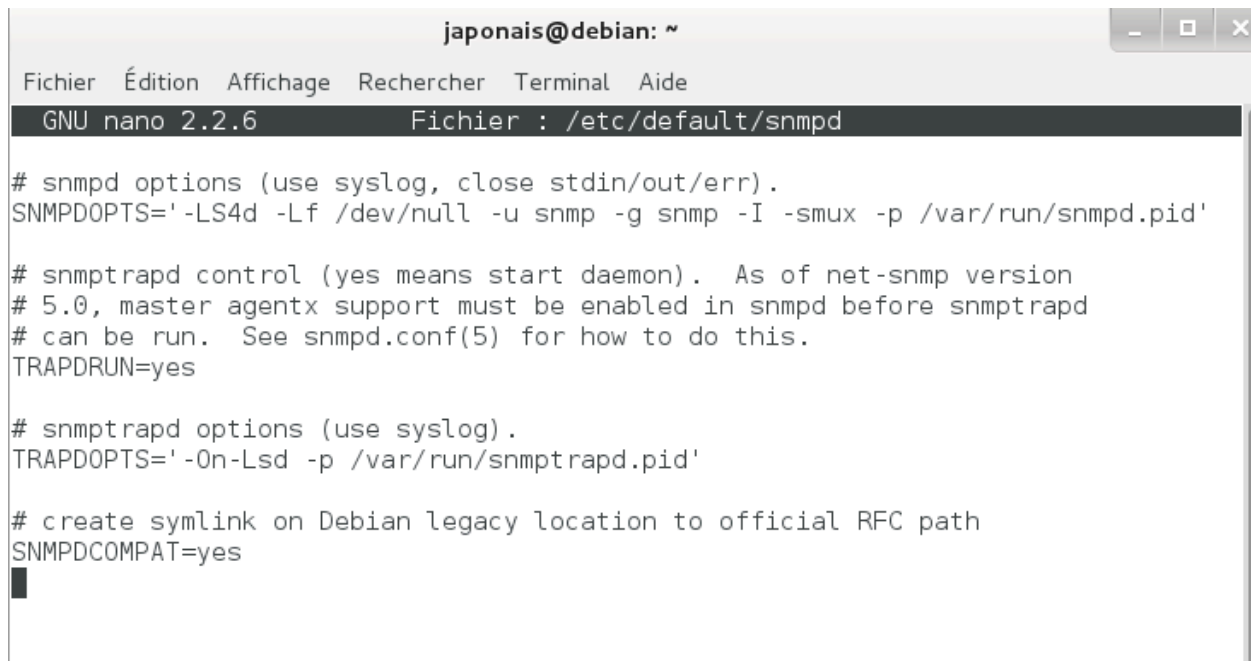
Modification du fichier /etc/snmp/snmpd.conf :

```
agentAddress udp::161  
.....  
rocommunity public localhost  
  
.....  
trapsink localhost public  
  
.....  
iquerySecName internalUser
```

Réduction des logs et pour recevoir les traps, modification du fichier /etc/default/snmpd :

```
# snmpd options (use syslog, close stdin/out/err).  
SNMPDOPTS='-LS4d -Lf /dev/null -u snmp -g snmp -I -smux -p /var/run/snmpd.pid' .....  
TRAPDRUN=yes  
  
.....  
# snmptrapd options (use syslog).  
TRAPDOPTS='-On -Lsd -p /var/run/snmptrapd.pid'
```

Le fichier `/etc/default/snmpd` après modification:



```
japonais@debian: ~
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
GNU nano 2.2.6      Fichier : /etc/default/snmpd

# snmpd options (use syslog, close stdin/out/err).
SNMPDOPTS='-LS4d -Lf /dev/null -u snmp -g snmp -I -smux -p /var/run/snmpd.pid'

# snmptrapd control (yes means start daemon).  As of net-snmp version
# 5.0, master agentx support must be enabled in snmpd before snmptrapd
# can be run.  See snmpd.conf(5) for how to do this.
TRAPDRUN=yes

# snmptrapd options (use syslog).
TRAPDOPTS='-On-Lsd -p /var/run/snmptrapd.pid'

# create symlink on Debian legacy location to official RFC path
SNMPDCOMPAT=yes
```

· Les librairies GD: **apt-get install libgd2-xpm-dev**

De nombreuses autres librairies

· Rrdtool : **# apt-get install rrdtool ;**

· Php-pear : **# apt-get install php-pear ;**

· Libraries Perl : **# apt-get install libperl-dev;**

Paquets divers: **apt-get install bsd-mailx lsb-release**

Redémarrons et testons apache2

Redémarrage de apache : **prompt# /etc/init.d/apache2 restart**

• Le serveur NTP: **apt-get install ntp**

Nous allons ensuite éditer la configuration comme suit:

Ajoutons les serveurs ntp de notre choix :

**server 0.fr.pool.ntp.org**

**server 1.fr.pool.ntp.org**

**server 2.fr.pool.ntp.org**

---

**server 3.fr.pool.ntp.org**

Redémarrer le serveur:

```
/etc/init.d/ntp restart
```

Création de l'utilisateur Nagios et définition du mot de passe.

```
# /usr/sbin/useradd Nagios
```

```
# passwd Nagios «EPB2015»
```

Création d'un groupe pour l'utilisateur nagios

```
# /usr/sbin/groupadd nagiosgrp
```

Faisons de l'utilisateur Nagios un membre de nagiosgrp

```
# /usr/sbin/usermod -G nagiosgrp Nagios
```

faire la même chose pour l'utilisateur d'apache

```
# /usr/sbin/usermod -G nagiosgrp www-data
```

Notre système est maintenant prêt à recevoir Nagios.

## **I.2 Installation du noyau Nagios**

Téléchargement de Nagios à partir du site officiel de nagios

```
# wget http://sourceforge.net/projects/nagios/files/nagios-3.x/nagios-3.5.1/nagios-3.5.1.tar.gz
```

Copier le fichier dans le répertoire /usr/src/

```
# cp /home/Téléchargement/Nagios-3.5.1 /usr/src/
```

Mettons nous dans /usr/src/ pour décompresser l'archive.

```
# tar xzf nagios-3.5.1.tar.gz
```

Rendons nous dans le dossier ainsi crée et compilons les sources

```
# cd Nagios-3.5.1
```

```
# ./configure --prefix=/usr/local/nagios --with-nagios-user=nagios --with-nagios-group=nagios --with-command-user=nagios --with-command-group=nagcmd --enable-event-broker --enable-nanosleep --enable-embedded-perl --with-perlcache
```



---

```
# make all
```

```
# make install
```

```
# make install-init
```

```
# make install-commandmode
```

```
# make install-config
```

Installation du script de démarrage

```
# ln -s /etc/init.d/Nagios /etc/rcS.d/S99nagios
```

Installations de l'interface web

```
# make install-webconf
```

Création du compte nagiosadmin qui se connectera à Nagios.

```
# htpasswd -c /usr/local/Nagios/etc/htpasswd.users nagiosadmin
```

redémarrage du serveur apache

```
#!/etc/init.d/apache2 restart
```

Cette commande demandera un mot de passe et nous saisirons celui que nous avons déjà attribué.

## I.3 Installation des plugins

### I.3.1 paquets nécessaires au fonctionnement des plugins

```
# apt-get install libgnutls-dev libssl-dev libkrb5-dev libldap2-dev libsnmp-dev gawk  
libwrap0-dev libmcrypt-dev smbclient fping gettext dnsutils libmysqlclient-dev
```

Nous installons maintenant les plugins requit pour que Nagios fonctionne. Nous devons d'abord récupérer les sources des plugins sur le site de Nagios ou sur [www.sourceforge.net](http://www.sourceforge.net) ensuite déplacer les sources dans `/usr/src/`.

```
# wget http://nagios-plugins.org/download/nagios-plugins-2.0.3.tar.gz
```

```
# cp nagios-plugins-2.0.3.tar.gz /usr/src/
```

Décompression et compilation

```
# tar xzf nagios-plugins-2.0.3.tar.gz
```

```
# cd nagios-plugins-2.0.3
```

```
# ./configure --with-nagios-user=nagios --with-nagios-group=nagios --prefix=/usr/  
local/nagios/ --enable-perl-modules --with-openssl=/usr/bin/openssl
```

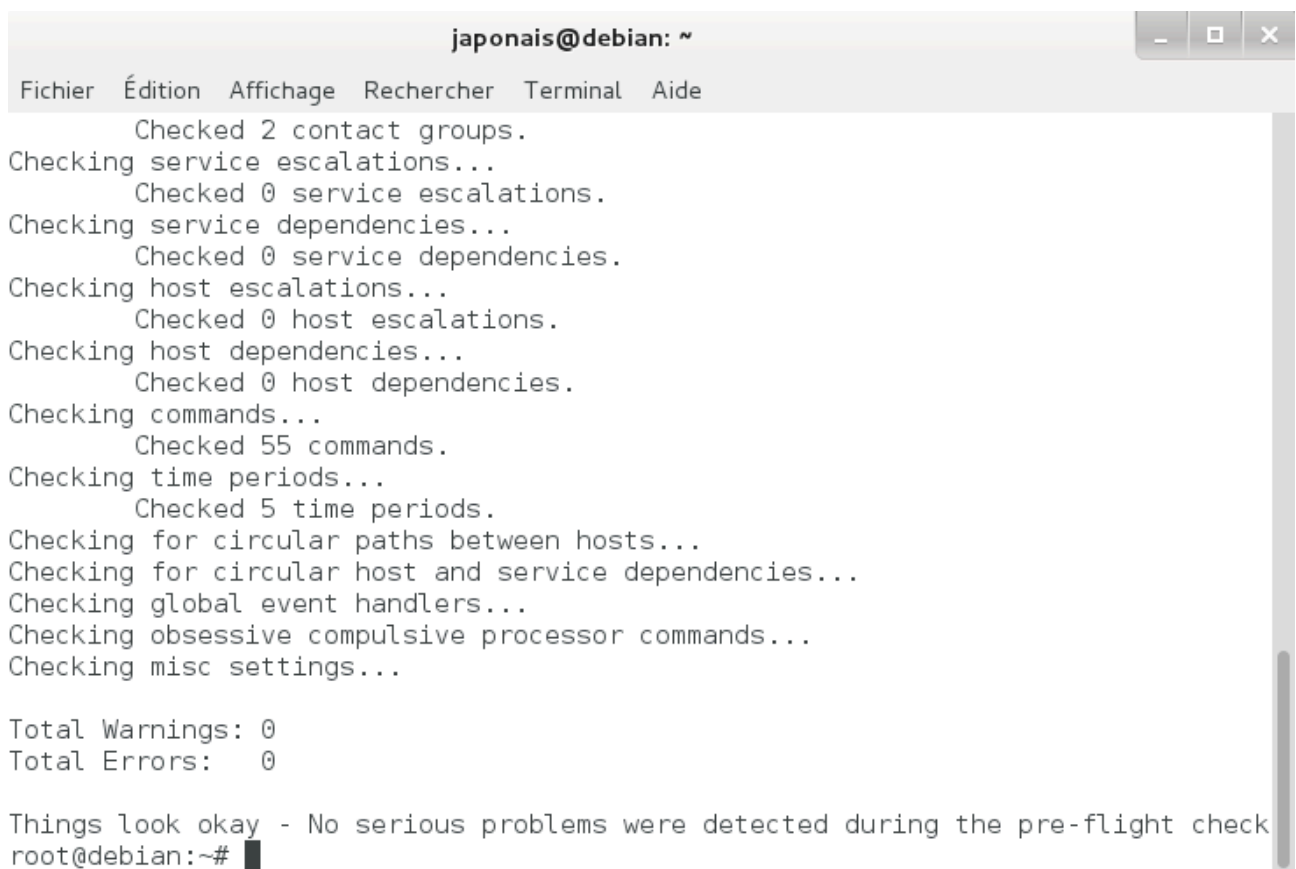
```
# make all
```

```
# make install
```

L'installation de Nagios est terminée pour le moment et reste plus qu'à vérifier la configuration avec la commande :

```
# usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
```

on doit avoir:



```
japonais@debian: ~  
Fichier  Édition  Affichage  Rechercher  Terminal  Aide  
Checked 2 contact groups.  
Checking service escalations...  
Checked 0 service escalations.  
Checking service dependencies...  
Checked 0 service dependencies.  
Checking host escalations...  
Checked 0 host escalations.  
Checking host dependencies...  
Checked 0 host dependencies.  
Checking commands...  
Checked 55 commands.  
Checking time periods...  
Checked 5 time periods.  
Checking for circular paths between hosts...  
Checking for circular host and service dependencies...  
Checking global event handlers...  
Checking obsessive compulsive processor commands...  
Checking misc settings...  
  
Total Warnings: 0  
Total Errors: 0  
  
Things look okay - No serious problems were detected during the pre-flight check  
root@debian:~#
```

### • explications des commandes:

==> **Make all** : Compiler les codes sources

**Make install** : Installer les binaires

**Make install-init** : Installer les scripts de démarrage

**Make install-config** : Installer les fichiers de configuration

**Make install-commandmode**: Installer et configurer les permissions

**Make install-webconf**: Installer les fichiers de configuration de Nagios dans le répertoire conf d'apache2.

Si des erreurs apparaissent lors de la compilation, nous devons revoir notre installation dès le début.

Donnons les droits à Nagios d'être propriétaire du répertoire `/usr/local/nagios/`

```
# chmod 774 /usr/local/nagios/*
```

```
# chown nagios:nagiosgrp /usr/local/nagios/*
```

```
# chown nagios:nagiosgrp /usr/local/nagios/*
```

On peut donc lancer notre navigateur, saisir l'adresse [http://Ip\\_Serveur/nagios/](http://Ip_Serveur/nagios/) ou <http://localhost/nagios/> et ceci après login.

En saisissant les bonnes coordonnées, la page d'accueil de Nagios s'ouvre.



**Figure A.1:** Page d'accueil de Nagios

Nagios dispose déjà d'une configuration par défaut, nous pouvons déjà superviser notre serveur. L'onglet « Host groups » dans le menu de gauche, nous permet de voir cela de plus près.

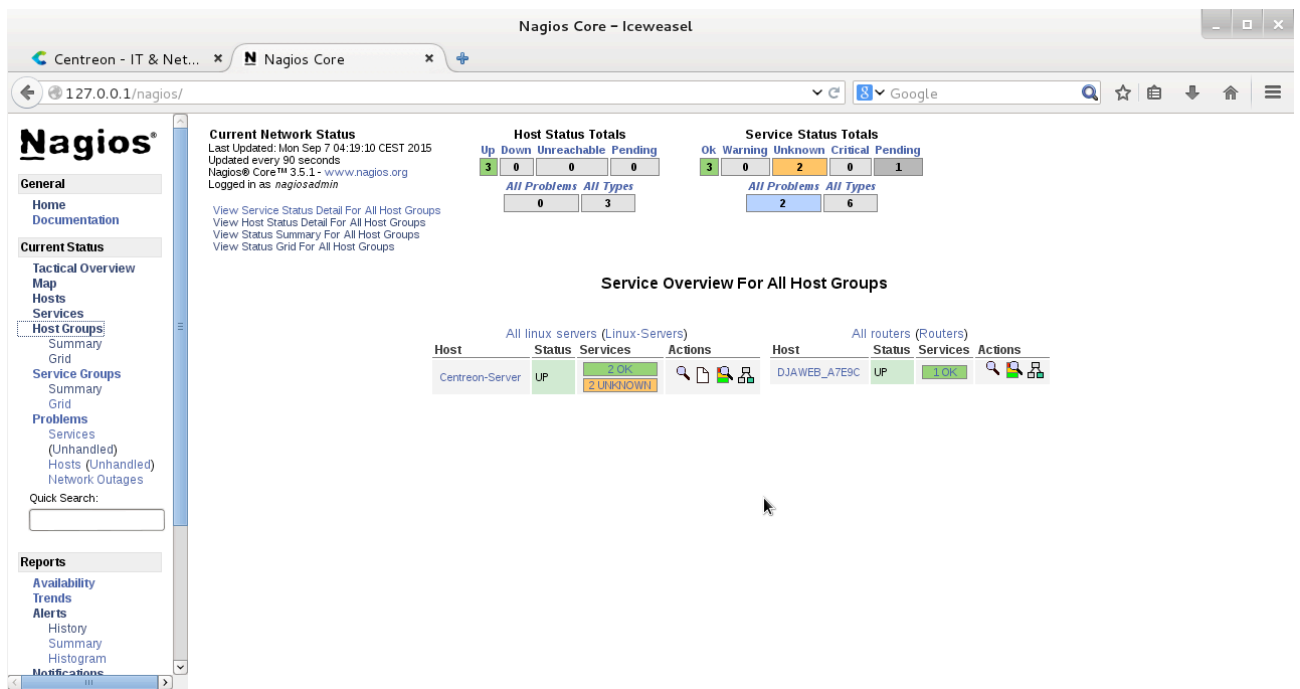


Figure A.2: Host group

Host= Nom de l'hôte, Status= état de l'hôte, Services= Nombre de services supervisé et leur état Actions.

## II. Installation de Centreon et Ndotools

Pour que la communication entre Nagios et Centreon soit établie, nous devons créer la base de données «ndo» et utiliserons le plugin NDOUtils.

### II.1 Installation des pré-requis nécessaires :

Création de la base de données ndo

```
# mysqladmin -u root -p create ndo
# mysql -u root -p mysql
mysql> GRANT ALL ON ndo.* TO "ndouser"@"localhost" IDENTIFIED BY
"ndopassword";
Query OK, 0 rows affected (0.00 sec)
mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.00 sec)
mysql> exit
```

### II.2 Installation de NDOutils

Téléchargement et compilation des sources de NDOUtils

---

Nous devons d'abord nous rendre sur le dossier

```
# Cd / usr / src /  
# Wget http://downloads.sourceforge.net/project/nagios/ndoutils-1.x/  
ndoutils-1.5.2/ndoutils-1.5.2.tar.gz  
# tar xzf ndoutils-1.5.2.tar.gz  
# Cd ndoutils-1.5.2  
# ./configure --prefix=/usr/local/nagios/ --enable-mysql --disable-pgsql --with-  
mysql-lib=/usr/lib/mysql/  
# Make  
# Cp src / ndomod-3x.o /usr/local/nagios/bin/ndomod.o  
# Cp src / ndo2db-3x / usr / local / nagios / bin / ndo2db
```

Modifions le fichier de Nagios sur ces deux ligne:

```
# nano /usr/local/nagios/etc/nagios.cfg  
event_broker_options = -1
```

**remarque:** il faut faire attention, la ligne suivante s'écrit sur une seule ligne.

```
broker_module = /usr/local/nagios/bin/ndomod.o config_file = /usr/local/  
nagios/etc/ndomod.cfg
```



```
japonais@debian: ~  
Fichier Édition Affichage Rechercher Terminal Aide  
GNU nano 2.2.6 Fichier : /usr/local/nagios/etc/nagios.cfg  
obsess_over_services=0  
process_performance_data=1  
service_perfddata_command=process-service-perfdata  
service_perfddata_file_mode=2  
check_for_orphaned_services=0  
check_for_orphaned_hosts=0  
check_service_freshness=1  
date_format=euro  
illegal_object_name_chars=~!$%^&*"'<>?,()=  
illegal_macro_output_chars=~$^&"|'<>  
admin_email=admin@localhost  
admin_pager=admin  
event_broker_options=-1  
debug_level=0  
debug_verbosity=2  
roker_module=/usr/local/nagios/bin/ndomod.o config_file=/usr/local/nagios/etc/$  
check_for_updates=0
```

## # Cp config / ndomod.cfg / usr / local / nagios / etc /

Modifions le fichier ndomod.cfg:

```
japonais@debian: ~
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
GNU nano 2.2.6  Fichier : /usr/local/nagios/etc/ndomod.cfg

#####
#
#       Last modification December 9, 2015, 6:56 am
#       By brahimi_yacine
#
#####

instance_name=Central
output_type=unixsocket
output=/usr/local/nagios/var/ndo.sock
tcp_port=5668
output_buffer_items=5000
buffer_file=/usr/local/nagios/var/ndomod.tmp
file_rotation_interval=14400
file_rotation_timeout=60
reconnect_interval=15
reconnect_warning_interval=900
data_processing_options=-1
config_output_options=3

^G Aide      ^O Écrire    ^R Lire fich.^Y Page préc.^K Couper     ^C Pos. cur.
^X Quitter   ^J Justifier ^W Chercher  ^V Page suiv.^U Coller    ^T Orthograp.
```

```
japonais@debian: ~
Fichier Édition Affichage Rechercher Terminal Aide
GNU nano 2.2.6 Fichier : /usr/local/nagios/etc/ndomod.cfg

tcp_port=5668
output_buffer_items=5000
buffer_file=/usr/local/nagios/var/ndomod.tmp
file_rotation_interval=14400
file_rotation_timeout=60
reconnect_interval=15
reconnect_warning_interval=900
data_processing_options=-1
config_output_options=3
█

^G Aide      ^O Écrire    ^R Lire fich.^Y Page préc.^K Couper    ^C Pos. cur.
^X Quitter   ^J Justifier ^W Chercher  ^V Page suiv.^U Coller   ^T Orthograp.
```

Rattrapons les droits sur les fichiers:

```
# Chmod 774 /usr/local/nagios/bin/local/ndo *
# Chown nagios:nagiosgrp /usr/local/nagios/bin/*
# Chown nagios:nagiosgrp /usr/local/nagios/etc/ndo *
```

Initialisons La base de données:

```
# ./installdb -u Nagios nagios h localhost -p -d ndo
```

Automatisons le lancement de ndo2db pour qu'il se lance au démarrage du serveur en créant le fichier /etc/init.d/ndo2db et en y copiant le script d'initialisation de Nagios :

```
# cp daemon-init /etc/init.d/ndo2db
```

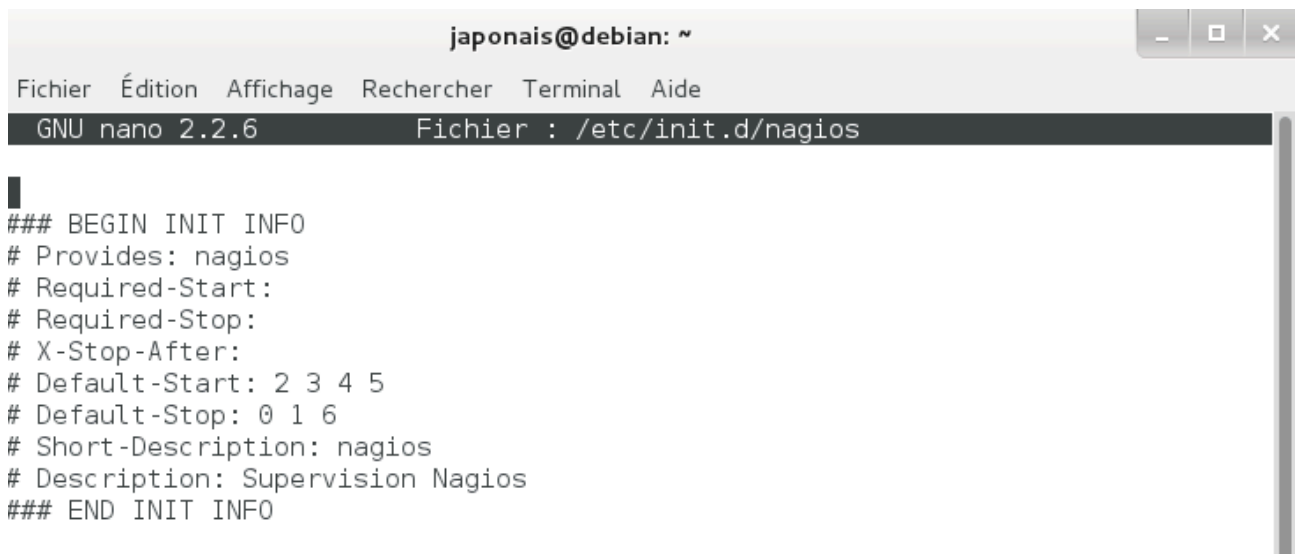
Ajoutons les lignes ci-dessous au début du fichier /etc/init.d/nagios:

```
### BEGIN INIT INFO
# Provides: nagios
# Required-Start:
# Required-Stop:
# X-Stop-After:
```

```
# Default-Start: 2 3 4 5
# Default-Stop: 0 1 6
# Short-Description: nagios
# Description: Supervision Nagios
```

```
### END INIT INFO
```

Le fichier /etc/init.d/nagios après modification:



```
japonais@debian: ~
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
GNU nano 2.2.6  Fichier : /etc/init.d/nagios

### BEGIN INIT INFO
# Provides: nagios
# Required-Start:
# Required-Stop:
# X-Stop-After:
# Default-Start: 2 3 4 5
# Default-Stop: 0 1 6
# Short-Description: nagios
# Description: Supervision Nagios
### END INIT INFO
```

Rendons le exécutable

```
# chown root:root /etc/init.d/ndo2db
```

```
# chmod 755 /etc/init.d/ndo2db
```

```
# update-rc.d ndo2db
```

```
# /etc/init.d/ndo2db start
```

Relançons Nagios:

```
# /etc/init.d/nagios restart
```

## II.3 Installations de Centreon

Télécharger les sources de Centreon depuis le lien

```
# wget http://downloads.centreon.com/index.php?id=144
```

Déplacer Centreon dans /usr/src/

```
# cp /home/Téléchargement/centreon-2.6.0.tar.gz /usr/src/
```

Allons décompresser l'archive.



---

```
# tar zxvf Centreon-2.6.0.tar.gz
```

```
# cd centreon-2.6.0
```

Lançons l'assistant en répondant à toutes les questions, qui sont régulièrement des confirmations de répertoire

```
# ./install.sh -i
```

```
...
```

```
you accept GPL license ? [y/n], default to [n]:
```

```
>y
```

```
Do you want to install : Centreon Web Front [y/n], default to [n]:
```

```
>y
```

```
Do you want to install : Centreon Nagios Plugins [y/n], default to [n]:
```

```
>y
```

```
Do you want to install : Centreon Snmp Traps process [y/n], default to [n]:
```

```
>y
```

```
Do you want me to create this directory ? [/usr/local/centreon] [y/n], default to [n]:> y
```

```
Path /usr/local/centreon OK
```

```
Do you want me to create this directory ? [/etc/centreon] [y/n], default to [n]:> y  
/usr/local/nagios/bin/nagios OK
```

```
Where is your NDO ndomod binary ? default to [/usr/sbin/ndomod.o]>
```

```
/usr/local/nagios/bin/ndomod.o OK
```

```
Do you want me to configure your sudo ? (WARNING) [y/n], default to [n]:> y  
Configuring Sudo OK
```

```
Do you want to add Centreon Apache sub configuration file ? [y/n], default to [n]:> y
```

```
Create „/etc/apache2/conf.d/centreon.conf“ OK
```

```
Configuring Apache OK
```

```
Do you want to reload your Apache ? [y/n], default to [n]:> y
```

```
Reloading Apache service OK
```

---

Do you want me to create this directory ? [/var/run/centreon] [y/n], default to [n]:> y

Path /var/run/centreon **OK**

Do you want me to create this directory ? [/var/lib/centreon] [y/n], default to [n]:> y

Path /var/lib/centreon **OK**

Do you want me to install CentStorage init script ? [y/n], default to [n]:> y  
CentStorage init script installed **OK**

Do you want me to install CentStorage run level ? [y/n], default to [n]:> y

Do you want me to install CentCore init script ? [y/n], default to [n]:> y  
CentCore init script installed **OK**

Do you want me to install CentCore run level ? [y/n], default to [n]:> y

Do you want me to create this directory ? [/var/lib/centreon/centplugins] [y/n], default to [n]:> y

Path /var/lib/centreon/centplugins **OK**

```
Backup all your snmp files                                OK
Change macros for snmptrapd.conf                         OK
Change macros for snmpptt.ini                           OK
Install : snmptrapd.conf                                 OK
Install : snmp.conf                                     OK
Install : snmpptt.ini                                   OK
Install : snmpptt                                       OK
Install : snmppttconvertmib                             OK
Create /etc/centreon/instCentPlugins.conf               OK
#####
#
#   Go to the URL : http://your-server/centreon/         #
#                   to finish the setup                 #
#
#   Report bugs at http://trac.centreon.com              #
#
#   Thanks for using Centreon.                           #
#   -----                                             #
#   Contact : infos@centreon.com                         #
#               http://www.centreon.com                  #
#
#####
```

Reste ainsi qu'à poursuivre l'installation de Centreon de via l'interface web en ouvrant notre navigateur et en tapant <http://localhost/centreon/> puis suivre l'assistant.

---

Centreon ainsi installé, il dispose d'une interface plus interactive et à travers celle-ci nous pouvons désormais manipuler Nagios plus aisément( ajout d'hôte, de service, alerte,...etc).

On doit tout d'abord rattraper les droits sur le répertoire **/usr/local/nagios/etc/**

```
# chmod -R 774 /usr/local/nagios/etc
```

Puis se rendre dans configuration/nagios/export, tout en veillant à ne pas avoir d'erreurs.

```
# /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
```

Notre serveur est ainsi configuré et fonctionne normalement.

## **II.4 Installation de SSH**

```
# apt-get install ssh
```

Nous empêcherons le login avec le compte « root » et modifiant le fichier **/etc/ssh/sshd\_config**

Désormais, notre serveur acceptera des connexions via ssh depuis tous les postes du réseau.

---

## Annexe B

### V. Installation de NSClient

#### • Partie Serveur (Machine Windows Distante)

Il faudra installer et configurer NSClient++ sur le serveur Windows

- Télécharger la version NSClient-0.3.8.75.
- Décompressez le client sous le répertoire C:\NSClient++-Win32-0.3.8.
- Ouvrir une commande DOS (cmd.exe)
- Entrer les commandes suivantes :

```
C:\cd NSClient++-Win32-0.3.8
```

```
C:\cd NSClient++-Win32-0.3.8\NSClient++.exe/install
```

L'installation est donc achevée, vérifions donc que le service est autorisé à "Interagir avec le bureau" (marquer Local system account et Allow service to interact with desktop dans l'onglet « Log On » du gestionnaire de service) en ouvrant le gestionnaire des services.

- Nous passons maintenant à la modification du fichier de configuration sous c://nscient/NSC.INI. Nous devons décommenter dans la première section [modules] tout les modules sauf CheckWMI.dll et RemoteConfiguration.dll
- Décommentons la ligne allowed\_hosts dans la section [Settings] et ajoutant l'adresse du serveur Nagios aussi pour des mesure de sécurité on a la possibilité d'attribuer un mot de passe pour accéder à NSClient.
- Démarrage NSClient:  
C:\cd NSClient++-Win32-0.3.8\NSClient++.exe/start
- Arrêt NSClient  
C:\cd NSClient++-Win32-0.3.8\NSClient++.exe/stop

#### • Partie Client (serveur Nagios)

Nous devons vérifier l'existence de la commande check\_nt sous /usr/local/nagios/libexec.

==>À travers l'invité de commande, testons si la machine Windows distante

---

```
#cd /usr/local/nagios/libexec  
#!/check_nt -H 62.245.223.181 -s admin -p 12489 -v CLIENTVERSION  
NSClient++ 0.3.8.75
```

==>la machine Windows distante à superviser est prête pour être supervisée. On ajoute la machine au serveur Nagios pour récupérer les informations nécessaires à l'aide de la commande check\_nt qui permet d'interroger à distance l'agent NSClient.

---

## Annexe C

### VI. Installation de NRPE

- **Partie Cliente (Serveur Linux)**

Nous devons maintenant accéder au serveur Linux à superviser en mode super utilisateur (root) et suivre les étapes suivantes :

- Création d'un utilisateur et groupe.

```
# cd /usr/sbin
# useradd nagios

# passwd nagios
# groupadd nagios
# usermod -G nagios nagios
```

- **Paquets nécessaires au fonctionnement des plugins:**

```
# apt-get install libgnutls-dev libssl-dev libkrb5-dev libldap2-dev libsnmp-dev gawk
libwrap0-dev libmcrypt-dev smbclient fping gettext dnsutils libmysqlclient-dev
```

- Téléchargement, décompression et installation des plugins Nagios, Nagios-plugins-2.0.3

```
# mkdir downloads
#cd downloads
#wget http://nagios-plugins.org/download/nagios-
plugins-2.0.3.tar.gz

# tar xzf nagios-plugins-2.0.3.tar.gz
#cd nagios-plugins-2.0.3
#./configure --with-nagios-user=nagios --with-nagios-
group=nagios --prefix=/usr/local/nagios/ --enable-perl-
modules --with-openssl=/usr/bin/openssl

#make
#make install
#chown nagios.nagios /usr/local/nagios
#chown -R nagios.nagios /usr/local/nagios/libexec
```

- Téléchargement, décompression et installation du plugin nrpe-2.15

```
# wget http://sourceforge.net/projects/nagios/files/nrpe-2.x/nrpe-2.15/nrpe-2.15.tar.gz #tar xzf nrpe-2.12.tar.gz
#cd nrpe-2.12
#./configure

#make

#make all
#make install-plugin
#make install-daemon #make install-daemon-config
```

- L'installation est terminée, passons donc à la configuration de /usr/local/nagios/etc/nagios/nrpe.cfg.

```
Allowed_host = @ du serveur nagios
```

Et rajouter la ligne suivante dans /etc/services :

```
nrpe 5666/tcp # NRPE
```

Enfin lancer le deamon XINETD relatif à NRPE :

```
# /etc/init.d/xinetd start
```

On peut aussi utiliser les commandes suivante:

```
#/etc/init.d/xinetd restart pour redémarrer
```

```
#/etc/init.d/xinetd stop pour stoppé
```

```
#/etc/init.d/xinetd status pour voir l'état de xinetd (stoppé ou démarré)
```

---

## Au niveau du serveur Nagios

Au niveau du serveur serveur Nagios, on refait les mêmes étapes pour l'installation de NRPE.

- Les plugins sont déjà installés.
- Téléchargement, décompression et installation du plugin nrpe-2.15.

```
#wget http://sourceforge.net/projects/nagios/files/nrpe-2.x/nrpe-2.15/nrpe-2.15.tar.gz
#tar xzf nrpe-2.15.tar.gz
#cd nrpe-2.15
#./configure --with-ssl=/usr/bin/openssl --with-ssl-lib=/usr/lib/x86_64-linux-gnu/ --libexecdir=/usr/local/nagios/libexec/
#make all
#make install-plugin
#make install-daemon
#make install-daemon-config
#make install-xinetd
```

Nous pouvons maintenant lancer le daemon XINETD relatif à NRPE :

```
# /etc/init.d/xinetd start
```

Depuis le terminal du serveur nagios testons si la machine Windows distante répond en tapant la commande suivante qui doit renvoyer la version de NSClient++ installée :

```
# cd /usr/local/nagios/libexec
#./check_nrpe -H @serveur-distant
```



---

## Annexe D

### VII. Notification par mail

#### VII.1 Définitions

- **Serveur SMTP**

Serveur smtp signifie protocole simple de transfert de courrier en français. Il est utilisé pour la gestion du transfert du courrier électronique vers les différents serveurs de messagerie électronique. De plus, il permet l'envoi d'email à partir des ordinateurs clients. la spécification d'un serveur pop et d'un serveur smtp lors de la configuration du logiciel du mail est importante.

- **Postfix**

Il est chargé d'envoyer les notifications vers votre serveur de messagerie.

- **Mailx**

il permet de tester l'envoi des emails

#### VII.2 Installations

- Installation de mailx et postfix depuis les sources, à travers la commande

```
# Apt-get install mailx, postfix
```

#### VII.3 Configuration :

Modification du fichier /etc/postfix/mail.cfg avec les adresses de la station de surveillance :

```
myhostname = localhost.localdomain localhost debian
mydestination = localhost.localdomain localhost debian
relayhost = 192.168.1.252
mynetworks=172.0.0.1
```

- **Myhostname** : Le nom du myhostname doit être le même que le nom de votre machine (nom qu'on retrouve dans /etc/hosts ou /etc/hostname).
- **Le mydestinitation** : identique au myhostname. si ces deux valeur sont différentes, le serveur ne pourra pas envoyer les emails de notifications .

- 
- **relayhost** : sert à renseigner l'IP ou le nom DNS du serveur de messagerie utiliser pour router votre courrier.
  - **mynetworks**: l'adresse de notre réseau.

Nous devons modifier depuis l'interface de centreon dans Configuration>command>notifications on modifie le script de « host-notify-by-email » et « service-notify-by-email » en y ajoutant la commande de test « mail » à la place @MAIL@ :

---

## Bibliographie

- [1] PUJOLLE, GUY, «Les Réseaux», 6ème édition, EYROLLES, 2008, Disponible sur: «<http://www.slideshare.net/JeromeYounan/les-reseaux-guy-pujolle-eyrolles-6me-ed-2008>»
- [2] Xavier Lasser, Thomas Klein et \_SebF. Réseaux Privés Virtuels-VPN [en ligne]. (15/02/2004, date de mise à jour: 15/01/2007) Disponible sur «<http://www.frameip.com/vpn/#3> - [Protocoles utilisés pour réaliser une connexion Vpn](#)»
- [3] Jacques CONION/ Cyril MAUBRY. Les VPN IP [en ligne]. Lille, 2001. Disponible sur: «<https://wapiti.telecom-lille.fr/commun/ens/peda/options/st/rio/pub/exposes/exposesrio2001/Conion-Maubry/12f.htm>»
- [4] Xavier Lasser, Thomas Klein et \_SebF. Réseaux Privés Virtuels-VPN [en ligne]. (15/02/2004, date de mise à jour: 15/01/2007) Disponible sur: «<http://www.frameip.com/vpn/#3.5.1> - [Principe de fonctionnement de Mpls](#)»
- [5] Jacques CONION/ Cyril MAUBRY. Les VPN IP [en ligne]. Lille, 2001. Disponible sur: «<https://wapiti.telecom-lille.fr/commun/ens/peda/options/st/rio/pub/exposes/exposesrio2008-ttnfa2009/Fort-Gengembre/mpls.html>»
- [6] eTutoriels.org. Overlay and peer to peer Model [en ligne]. (2008, date de mise à jour 2015) Disponible sur: «<http://etutorials.org/Networking/MPLS+VPN+Architectures/Part+2+MPLS-based+Virtual+Private+Networks/Chapter+7.+Virtual+Private+Network+VPN+Implementation+Options/Overlay+and+Peer-to-peer+VPN+Model/>»
- [7] Nouchti Ouafa, EL QASMI Med Zakaria, HILALI Tarik. Etude comparative et réalisation d'un VPN MPLS [en ligne]. Réseaux et Télécoms. Maroc: Ecole Marocaine des sciences de l'ingénieur, 2009/2010. Disponible sur: «<https://fr.scribd.com/doc/58133240/vpn-mpls-GNS3#scribd>»
- [8] Xavier Lasser, Thomas Klein et \_SebF. Réseaux Privés Virtuels-VPN [en ligne]. (15/02/2004, date de mise à jour: 15/01/2007) Disponible sur: «<http://www.frameip.com/vpn/#4.5> - [Mpls / IPSec](#)»
- [9] Asmaa KSIKS, Ismaël MAIGA. Etude et simulation sur GNS3 du service MP-BGP/VPN-IP [en ligne]. Génie Réseaux et Télécoms. Marrakech, Maroc: Ecole Nationale des sciences Appliquées de Marrakech, 2010/2011. Disponible sur: «<http://www.fichier-pdf.fr/2013/05/07/rapport-mpls-vpn-ip/preview/page/1/>»
- [10] Bastien MIGETTE. Blog sur les technologies réseau et sécurité [en ligne]. (10/12/2008) Disponible sur : «<http://www.bmigette.fr/2008/12/10/mpls-vrfs-bgp-pour-sammuser/>»
- [11] CISCO. Configuration d'un VPN MPLS de base [en ligne]. Disponible sur : «[http://www.cisco.com/cisco/web/support/CA/fr/109/1093/1093293\\_mpls\\_vpn\\_basic.html](http://www.cisco.com/cisco/web/support/CA/fr/109/1093/1093293_mpls_vpn_basic.html)»
- [12] Julien BERTON. Mise en place d'un VPN MPLS [en ligne]. (01/01/2012). Disponible sur: «<http://ccie.julienberton.fr/2012/01/01/mise-en-place-dun-vpn-mpls/>»
- [13] Elie MABO, Amadou NIANG. La supervision avec NAGIOS [en ligne] Sécurité des système informatique. Rouen, FRANCE: Université de ROUEN, Janvier 2009. Disponible sur : «<http://www.doc->

---

[developpement-durable.org/file/Projets-informatiques/cours-&-manuels-informatiques/Nagios/La%20supervision%20avec%20Nagios-Centreon.pdf](http://developpement-durable.org/file/Projets-informatiques/cours-&-manuels-informatiques/Nagios/La%20supervision%20avec%20Nagios-Centreon.pdf)

[14] Site officiel de NAGIOS: «[www.nagios.org](http://www.nagios.org)»

[15] Othman Souli. Mise en place d'un système de supervision open source [en ligne]. TUNISIE: Université Virtuelle de Tunis. 2010/2011. Disponible sur: «[http://pf-mh.uvt.rnu.tn/573/1/Mise\\_en\\_place\\_d%E2%80%99un\\_sys%%C3%A8me\\_de\\_supervision\\_Open\\_source..pdf](http://pf-mh.uvt.rnu.tn/573/1/Mise_en_place_d%E2%80%99un_sys%%C3%A8me_de_supervision_Open_source..pdf)»

[16] Blog Nicolargo. Structure des fichiers de configuration de nagios 3 [en ligne]. Juin 2008. Disponible sur: «<http://blog.nicolargo.com/2008/06/structure-des-fichiers-de-configuration-de-nagios-3.html>»

[17] Ethan Galstad. Nagios Entreprises ,Documentation Nagios Version 3.x [en ligne]. Ed. Française Docbook. 1999-2007. Disponible sur: «[https://cloud.github.com/downloads/monitoring-fr/Documentation-Nagios-3.x-French/fr\\_FR.nagios-3.x-beta-8.pdf](https://cloud.github.com/downloads/monitoring-fr/Documentation-Nagios-3.x-French/fr_FR.nagios-3.x-beta-8.pdf)»

[18] Wiki Monitoring-fr.org. Nagios Centreon Part 2 [en ligne].(Modifié le 29/03/2013). Disponible sur: «<http://wiki.monitoring-fr.org/centreon/nagios-centreon-part2#explication-precises-des-interactions-entre-les-differents-services>»

[19] Site officiel de centreon: «[www.centreon.com](http://www.centreon.com)»

[20] linuxpedia.fr. Nagios et Centreon: Description des interactions [en ligne].(Modifié le : 09/05/2014). Disponible sur: «[http://www.linuxpedia.fr/doku.php/serveurs/nagios\\_centreon](http://www.linuxpedia.fr/doku.php/serveurs/nagios_centreon)»

[21] Wiki Monitoring-fr.org. Nagios Centreon Part 2 [en ligne].(Modifié le 29/03/2013). Disponible sur: «<http://wiki.monitoring-fr.org/centreon/manuel-utilisation/start>»

[22] Slim CHAKROUN, Emna BEN HADJ YAHIA, Safa GALLAH. Securiday Access Control . TUNISIE: Institut National des Sciences Appliquées et de Technologie. 26/04/2014. Disponible sur: «[http://www.securinets.com/sites/default/files/fichiers\\_pdf/securiday14/Monitoring\\_Securiday2014.pdf](http://www.securinets.com/sites/default/files/fichiers_pdf/securiday14/Monitoring_Securiday2014.pdf)»

[23] Jean-François PILLOU, CommentCaMarche.net, Le protocole SNMP. Disponible sur: «<http://static.ccm2.net/www.commentcamarche.net/contents/pdf/le-protocole-snm-537-nol400.pdf>»

## Résumé

Notre projet est constitué de deux parties distinctes:

La première partie, concerne la mise en place d'un réseau VPN a base de la technologie MPLS. L'objectif de notre travail consiste à proposer une architecture réseau sécurisée de l'Entreprise Portuaire de Béjaïa. Pour cela, nous avons étudié le réseau actuel, ce qui nous a permis de suggérer des solutions afin de proposer une nouvelle architecture plus sécurisée. Ensuite, nous avons présenté un aperçu du fonctionnement du MPLS, puis la configuration du réseau proposé à l'entreprise à l'aide du simulateur réseau GNS3.

La seconde partie, concerne la supervision du réseau de l'EPB. Dans cette étude, nous avons mis en place et configuré une station de surveillance Nagios chargée d'alerter l'administrateur en cas de pannes ou de surcharge sur le réseau. Nous avons configuré des programmes exécutables (plugins) et certaines extensions (NRPE et NSClient) qui permettent de surveiller les machines utilisant les systèmes d'exploitation LINUX et WINDOWS. Les différentes configurations sont faites sur une machine virtuelle utilisant le système d'exploitation LINUX.

**Mots clés: VPN, MPLS, GNS3, Nagios, Centreon, NRPE, NSClient.**

## Abstract

Our project consists of two distinct parts:

The first part concerns the creation of a VPN-based MPLS. The aim of our work is to provide a secure network architecture of the Port of Bejaia Company. For this, we studied the current network, which allowed us to suggest solutions in order to propose a new, more secure architecture. Then we presented an overview of the operation of MPLS and configuration of the proposed network to the company with the GNS3 Network simulator.

The second part concerns the supervision of the network of the EPB. In this study, we have implemented and configured a Nagios monitoring station to alert the administrator responsible in case of failures or overload on the network. We set up executable programs (plugins) and some extensions (ERS and NSClient) that monitor the machines using the LINUX and WINDOWS operating systems. The different configurations are made in a virtual machine running the LINUX operating system.

**Keywords: VPN, MPLS, GNS3, Nagios, Centreon, NRPE, NSClient.**