UNIVERSITE SIDI MOHAMED BEN ABDELLAH
FACULTÉ DES SCIENCES ET TECHNIQUES FÈS
DÉPARTEMENT D'INFORMATIQUE

FST FES

PROJET DE FIN D'ETUDES

MASTER SCIENCES ET TECHNIQUES
SYSTÈMES INTELLIGENTS & RÉSEAUX

MISE EN PLACE D'UN SERVEUR UNIFIED ACCESS GATEWAY, ET CONFIGURAATION DU LOGICIEL « NAGIOS » POUR LA SUPERVISION DU RÉSEAU WI-FI

LIEU DE STAGE : HCEFLCD ET AZ-NET

RÉALISÉ PAR : KAOUTAR ACHERKI

SOUTENU LE : 22 JUIN 2013

ENCADRÉ PAR :

M.MOHAMMAD CHAOUKI ABOUNAIMA
MME. ILHAM LAMRINI
M.HICHAM ANGHASS
M.ADEL ECHCHAAOUI

DEVANT LE JURY COMPOSÉ DE :

M.	A.ZAHI	(PRÉSIDENT)
M.	M.C.ABOUNAIMA	(FSTF)
M.	K.ABBAD	(FSTF)
M.	M.OUZARF	(FSTF)

ANNÉE UNIVERSITAIRE 2012-2013

Dédicace :

A mes chers PARENTS pour leur amour, leurs sacrifices et leur affection;

A mes chères SOEURS pour leur encouragement continu ;

A tous mes ami(e)s pour leur soutien ;

Qu'ils trouvent ici l'expression de mon affection et gratitude

Kaoutar ACHERKI

Remerciements

Au terme de ce travail, nous tenons à remercier vivement notre encadrant à la FSTF M. **Mohammad Chaouki ABOUNAIMA** pour ses précieuses directives et ses conseils tout au long du stage.

Nous remercions nos encadrant externes **M. Adel ECHCHAACHOUI** et **M .Hicham ANGHASS** pour leur disponibilité et leur précieux conseils.

Nous remercions vivement tous les membres du jury d'avoir accepté de juger notre travail.

Remerciements spéciaux à tout le corps professoral de la faculté des sciences et techniques Fès, qui nous ont accompagnés tout au long de notre formation.

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

ملخص

هذا التقرير هو عبارة عن ثمرة وخلاصة أربعة أشهر من التدريب بالمندوبية السامية للمياه والغابات ومحاربة التصحر، والشركة ازيدنت وذلك في إطار مشروع إعداد دراسة لنيل دبلوم الماستر.

نظرا إلى الأهمية التي يكتسيها أمن بنية الشبكات المعلوماتية ارتأينا ضرورة إعداد ملقم UAG لشبكة المندوبية السامية للمياه والغابات ومحاربة التصحر،هذا الملقم يعد بمثابة عبّارة للوصول البعيد الشيء الذي مكننا من خلق بوابة وتأمين المنشورات بداخلها.

من ناحية أخرى لمواكبة الثورة التي عرفتها الشبكة اللاسلكية خلال السنوات الأخيرة،كان لابد لنا من التعرف على بنية هذا النوع من الشبكات ولهذا، داخل شركة ازيدنت اخترنا تطوير البرنامج ناجيوس وبالتالي تمكنا من الحصول على نظرة عامة على اليات عمل الشبكة اللاسلكية .

يهدف هذا التقرير إلى شرح المنهج الذي اتخذناه طيلة مرحلة الإنجاز وأيضا مختلف الاختيارات التقنية المعتمدة، والتي أدت الى تحسين مصلحة المعلوميات بالمندوبية السامية للمياه والغابات ومحاربة التصحر، وكذا تطوير البرنامج ناجيوس للحصول على لمحة عامة عن سير وعمل الشبكة اللاسلكية داخل الشركة ازيدنت.

Résumé

Dans ce rapport, nous allons présenter le fruit de quatre mois de stage au sein du Haut-Commissariat aux eaux et Forêts et la Lutte Contre la Désertification et de l'entreprise AZ-Net. Ces quatre mois de stage s'inscrivent en fait dans le cadre de notre projet de fin d'étude.

Vu l'ampleur de la sécurité de l'infrastructure réseau au sein du Haut-Commissariat aux eaux et Forêts et la Lutte Contre la Désertification, nous avons mis en place un serveur UAG qui est une passerelle d'accès distant, permettant de créer un portail pour le réseau, et d'insérer des publications sécurisés dans ce dernier.

Aussi, dans l'optique d'élargir et d'approfondir nos connaissances en matière du fonctionnement des réseaux sans fil Wi-Fi qui sont devenus, aujourd'hui, omniprésents dans notre vie, nous avons opté pour configurer le logiciel « Nagios ».

Le présent rapport vise à expliquer la démarche que nous avons adoptée tout au long de la réalisation de ces deux projets ainsi qu'il met l'accent sur les différents choix techniques effectués, et qui ont permis d'une part l'amélioration du service informatique du HCELFCD et de l'autre part, un progrès au niveau du logiciel « Nagios ».

Abstract

In this report, we presented the results of four months of training within the High Commission for Water, Forests and Desertification Control and the company AZ-Net, which is part of our final project study.

Given the magnitude of the security of the network infrastructure in the High Commissioner for Water, Forests and Desertification Control, we set up a UAG server which is a gateway remote access to create a portal for the network, and mad this portal publications secured.

On the other hand, wireless networks Wi-Fi are now ubiquitous in our society, hence the need for a global view of these networks, this effect within company AZ-Net, this is why we opted modeled the "Nagios" software in order to have a global view of a Wi-Fi network.

This report aims to explain the approach we have adopted, as well as the various technical choices considered, which led to the improvement of IT service HCELFCD and even progress in the "Nagios" software for an overview of the Wi-Fi network within the company AZ-Net.

Sommaire

Introduction générale

De nos jours, le réseau est en train de devenir un passage obligatoire pour tous les domaines de la vie. Ainsi, la gestion des réseaux s'avère comme une tache indispensable et primordiale. D'ailleurs, Il faut souvent avoir recours à des techniques d'administration pour pouvoir contrôler le fonctionnement des réseaux et aussi pour exploiter au mieux les ressources disponibles afin de rentabiliser au maximum les investissements réalisés.

La gestion de réseaux informatiques, se réfère aux activités, méthodes, procédures et aux outils mis en œuvre par l'administrateur réseau et qui ont trait à l'exploitation, l'administration, la maintenance et la fourniture des réseaux informatiques et leur sécurité.

Elle constitue un problème dont l'enjeu est de garantir au meilleur coût, non seulement la qualité du service rendu aux utilisateurs mais aussi la réactivité due aux changements et à l'évolution rapide du secteur informatique.

D'ailleurs, la gestion des réseaux se définit comme étant l'ensemble des moyens mis en œuvre (connaissances, techniques, méthodes, outils, ...) pour superviser, exploiter des réseaux informatiques et planifier leur évolution en respectant les contraintes du coût, de qualité et de matériel. La qualité de service se décline sur plusieurs critères pour le futur utilisateur, notamment la disponibilité, la performance (temps de réponse), la fiabilité, la sécurité.

C'est pour cette raison que dans le cadre de notre formation du Master Sciences et Techniques Systèmes Intelligents & Réseaux à la faculté des sciences et techniques- à Fès nous avons opté pour travailler à la fois sur le sujet de la mise en place d'un serveur UAG et sur la modélisation du logiciel de supervision du réseau Wi-Fi open-source « Nagios ».

A cet effet, nous avons effectué un stage de fin d'étude de quatre mois au sein du Haut-Commissariat aux Eaux et Forêts et à la Lutte Contre la Désertification (HCEFLCD) et à l'entreprise AZ-Net. Ce stage nous a aidé à mener à bien notre réflexion sur la gestion réseaux. A travers ce travail appuyé par le stage de fin d'étude nous aspirons principalement

à valoriser la sécurité réseau par la mise en place d'un serveur UAG, ainsi que nous mettons l'accent sur la supervision wifi à travers la configuration du logiciel « Nagios ».

La première partie de ce travail, sera consacré à la mise en place d'un serveur UAG. Ainsi, nous allons mettre l'accent tout d'abord, sur l'organisme d'accueil, le cahier des charges et la gestion du projet. Ensuite, nous établirons un aperçu général sur l'UAG. Enfin, nous allons exposer les différentes étapes de la mise en place de la plateforme relatives à notre projet.

Et la deuxième partie, traite la configuration du logiciel « Nagios » afin de pouvoir superviser le réseau Wi-Fi y afférant. Pour élucider les propriétés de ce projet et ses étapes d'une part, nous allons commencer par une présentation de l'organisme d'accueil et du contexte général du projet et de l'autre part, nous allons mettre l'accent sur la planification du projet. Les généralités sur le réseau Wi-Fi et le logiciel « Nagios » fera l'objet du deuxième chapitre. Alors que, le troisième chapitre sera consacré aux étapes d'installation de « Nagios » et sa modélisation.

Pour conclure, nous allons mettre en avant des recommandations et des propositions pour une éventuelle amélioration.

Les dernières pages de notre rapport seront consacrées à présenter l'annexe et une liste des abréviations utilisées dans ce rapport.

Partie I

Dans cette partie, nous allons aborder la mise en place d'un serveur UAG au sein du Haut-commissariat aux Eaux et Forêts et à la lutte contre la désertification.

Chapitre I

Etude de l'existant

I. L'organisme d'accueil

Avant d'entamer notre sujet, nous préférons de commencer par une brève présentation de l'institution qui nous a accueilli durant la première partie de notre stage.

Le Haut-Commissariat aux Eaux et Forêts et à la Lutte Contre la Désertification (HCEFLCD) est un organisme du gouvernement marocain jouissant de la pleine capacité juridique et de l'autonomie financière.

Cet institut siégeant à Rabat est chargé de préserver notre biodiversité en partant du principe disant que l'importance de la forêt repose sur sa valeur de patrimoine. Ainsi, le HCEFLCD se situe au cœur des politiques de gestion durable des milieux naturels et assure, dans cette optique, la mission de conservation, d'aménagement et de gestion des forêts et des milieux naturels.

L'HCEFLCD a pour missions de gérer neuf millions d'hectares d'espaces naturels, soit 12 % du territoire national et ce par le biais d'une planification des actions et des activités autour d'axes stratégiques que nous pouvons résumer dans les points suivants:

- Elaborer et mettre en œuvre la politique du gouvernement dans les domaines de la conservation et du développement durable des ressources forestières, alfatières, sylvo-pastorales dans les terrains soumis au régime forestier, ainsi que le développement cynégétique, piscicole continentale et des parcs et réserves naturelles ;

- Coordonner la mise en place des mécanismes institutionnels pour la préparation, l'exécution, le suivi et l'évaluation de la politique du gouvernement en matière de lutte contre la désertification ;

- Participer à l'élaboration et à la mise en œuvre de la politique du gouvernement en matière de développement rural.

- Assurer l'administration, par délégation de M. le Premier Ministre et conformément aux dispositions du dahir du 10 octobre 1917 sur la conservation et l'exploitation des forêts, tel qu'il a été modifié et complété, du domaine forestier de l'Etat et les autres biens soumis au régime forestier ainsi que la police et le contrôle de l'application des textes législatifs et réglementaires y afférents;

- Œuvrer à la promotion et à la mise en œuvre des actions d'extension et de développement de la forêt sur des terres à vocation forestière autres que celles du domaine forestier de l'Etat;

- Coordonner l'élaboration et la mise en œuvre des plans d'aménagement des bassins versants et des parcs et réserves naturelles et en assurer le suivi et l'évaluation en concertation avec les différents départements ministériels ou d'autres organismes concernés ;

- Coordonner la préparation et la mise en œuvre des programmes et projets de développement intégré des zones forestières et alfatières, participer à leur exécution et en assurer le suivi et l'évaluation.

I.1. Les administrations du HCEFLCD

Le Haut-Commissariat aux Eaux et Forêts et à la Lutte Contre la Désertification comprend, outre le cabinet du haut-commissaire, une administration centrale et des services déconcentrés.

- L'administration est composée des services suivants :

  - Le secrétariat général;
  - L'inspection générale;
  - la direction du domaine forestier, des affaires juridiques et du contentieux;

- La direction de la lutte contre la désertification et de la protection de la nature;
- La direction du développement forestier;
- La direction de la planification, du système d'information et de la coopération;
- La direction des Ressources Humaines et des Affaires Administratives;
- Le centre de recherche forestière.

- Les services extérieurs du HCEFLCD:

  - 10 Directions Régionales des Eaux et Forêts.
  - Le Parc zoologique National de Rabat.
  - Le Centre National d'Hydrobiologie et de Pisciculture d'Azrou.

I.2. Organigramme du HCEFLCD [1]

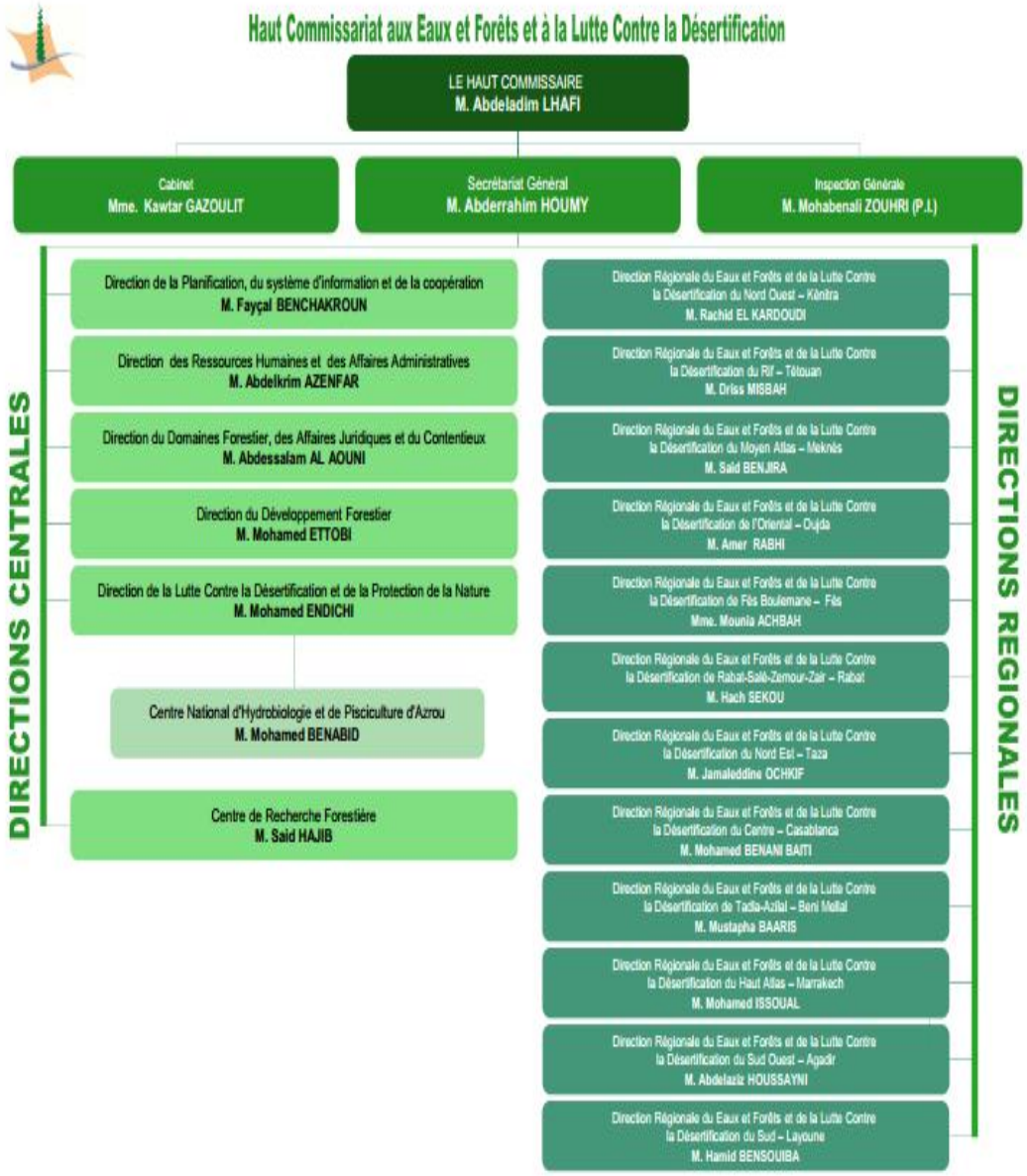

Figure n° 1 : Organigramme du HCEFLCD

[1] http://www.eauxetforets.gov.ma/files/editor_upload//organigramme-HCEFLCD.pdf

II. Cahier des charges

II.1. Présentation du projet

Unified Access Gateway (UAG) est conçu pour contrôler l'accès entrant aux ressources d'entreprise à partir de plusieurs types de clients tels que Windows, Linux, Macintosh, y compris les appareils mobiles. Un des avantages majeurs de Forefront UAG est la politique d'accès des terminaux. UAG peut être utilisé pour permettre aux clients l'accès aux ressources internes et ce seulement si un ensemble de règles prédéfinies par les administrateurs UAG sont satisfaits.

Forefront UAG fournit un soutien portail pour accéder aux ressources internes. Un portail est en fait un site Web où les utilisateurs peuvent accéder à différentes applications publiées comme OWA, les connexions Bureau à distance, VPN SSL, SharePoint et bien d'autres.

II.1.1. Intérêt du projet

Afin d'apporter une amélioration au système du Haut-Commissariat aux Eaux et Forêts et à la Lutte Contre la Désertification, il est demandé de concevoir un logiciel qui respecte la politique de sécurité du réseau, et qui permet en même temps aux employés en mobilité un accès au réseau interne. Pour les autres besoins de mobilité, nous souhaitons publier des applications web à diverses populations.

II.2. Etude de l'existant

II.2.1. Présentation du service informatique

Le Service Informatique est un service du Haut-Commissariat aux Eaux et Forêts et la Lutte Contre la Désertification. Il a pour principale mission la mise en place de la politique informatique du HCEFLCD.

Le Service Informatique est chargé aussi d'assurer plusieurs objectifs :

- Il implante et gère les moyens informatiques collectifs et les réseaux, à l'exclusion des équipements bureautiques. Il peut toutefois apporter, dans ce domaine, un conseil quant au choix des équipements.

- Il élabore et réalise le plan de formation des utilisateurs aux outils qu'il a mis en place.

- Il assure également une assistance technique aux utilisateurs des logiciels et des réseaux qu'il a implanté. Cette mission ne concerne que les services administratifs.

II.2.2. Architecture du système informatique

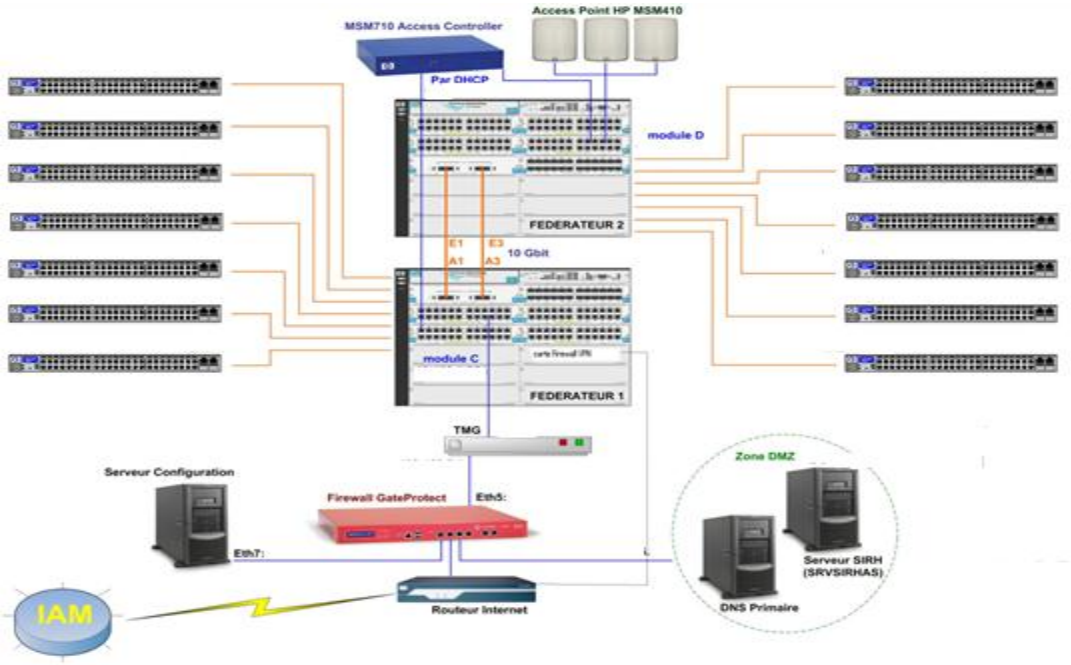

Figure n° 2 : Architecture du système informatique du HCEFLCD

La sécurité du système informatique du HCEFLCD est assurée par deux outils :

- GateProtect : un pare-feu matériel dit de " next génération Firewall", breveté et standardisé ISO 9241. Seul GateProtect a passé les certifications ISO sur le marché des firewalls. Ses principales fonctionnalités sont :

  - ⇨ Gestion graphique ;
  - ⇨ Firewall applicatif (facebook, skype...);
  - ⇨ Filtrage web;
  - ⇨ Détection d'intrusions ;
  - ⇨ Passerelle VPN ;

- ⇨ Antivirus de flux ;
- ⇨ Anti spam ;
- ⇨ Gestion de certificat ;
- ⇨ Chiffrement & Signature.

- Forefront TMG : un pare-feu logiciel qui protège le réseau interne de l'Internet et qui fournit un accès protégé à partir des ressources internes à Internet. Forefront TMG dispose de fonctionnalités d'édition puissantes pour publier des services internes à l'Internet tels qu'Outlook Web Access, Exchange Active Sync et un ensemble d'autres services.

II.3. Problématique

Afin de sécuriser l'infrastructure réseau, le HCEFLCD utilise un firewall logiciel « TMG » qui est une passerelle Web permettant aux entreprises d'utiliser Internet de façon sécurisée et efficace, sans crainte des logiciels malveillants ou d'autres menaces. Pour mieux bloquer les menaces récentes en provenance du Web, ce produit multiplie les couches de protection (filtrage d'URL, recherche de logiciels malveillants et prévention des intrusions) et les met à jour en permanence.

Bien que le « TMG » possède beaucoup d'avantage et qu'il se caractérise par sa performance. Mais des anomalies sont enregistrées au sein du HCEFLCD surtout au niveau de Microsoft. Ce derniere, ne produit plus sa licence depuis décembre 2012 ainsi qu'il arrête tout développement sur TMG et par conséquent il n'y aura plus de nouvelles fonctionnalités (pas de support d'IPv6, …) d'où la nécessité du recours à une autre solution firewall possédant les mêmes fonctionnalités du « TMG » et prenant en considération l'amélioration des défauts constatés.

II.4. Solutions proposées

Dans l'intention de trouver une solution à la problématique soulevée de la licence du firewall TMG, nous avons mis en place : Forefront Unified Access Gateway qui est un nouveau produit de Microsoft, regroupant l'ensemble des solutions de publication déjà existantes :

- Remote Desktop Gateway ;
- VPN ;
- Une nouvelle version d'Intelligent Access Gateway (IAG 2007) ;
- DirectAccess.

La principale différence entre TMG est UAG réside dans le niveau de sécurité. Autrement dit Forefront UAG apporte une couche de **sécurité applicative**. Vous trouvez ci-après un tableau présentant une comparaison entre TMG et la solution proposée : UAG :

	TMG	***UAG***
Support Windows server 2008 R2	X	X
Virtualisation de la solution	X	X
Haute disponibilité	X	X
Support publication Exchange 2010	X	X
Publication HTTP et HTTPS	X	X
Vérification de la conformité des postes		X
Profil d'accès aux applications		X
Publication d'application non web	X	X
Publication Remote Desktop		X
Portail d'application		X
SSO entre application publiées		X
Serveur Direct Access		X

Tableau n° 1: Tableau comparatif entre TMG et UAG

III. Planification du projet

III.1. Cycle de vie

Le « cycle de vie d'un logiciel », désigne toutes les étapes du développement d'un logiciel, de sa conception à sa disparition. L'objectif d'un tel découpage est de réaliser la définition des jalons intermédiaires permettant la validation du développement logiciel, c'est-à-dire assurer la conformité du logiciel avec les besoins exprimés, et la vérification du processus de développement visant d'atteindre l'adéquation des méthodes mises en œuvre.

III.1.1. Spécification des besoins

La spécification des besoins consiste à analyser et à évaluer les besoins à satisfaire, avec si possible leur hiérarchisation par ordre de priorité, elle nécessite la collection des données disponibles ainsi que la consultation de l'équipe du service informatique.

III.1.2. Analyse

Cette étape est consacrée à l'étude de tous les aspects de la mise en place du serveur « UAG » en vue de s'assurer de son fonctionnement et d'organiser tout le processus de sa mise en œuvre afin qu'il soit réalisé dans les délais voulus et qu'il atteigne les résultats attendus.

III.1.3. Installation et Configuration

Cette étape est axée sur la mise en place du logiciel « UAG » et sur sa configuration afin de pouvoir créer un portail pour le réseau et d'effectuer par conséquent des publications à travers ce dernier.

III.1.4. Test

Les tests permettent de vérifier individuellement si le logiciel « UAG » est implémentée conformément aux spécifications des besoins ou non.

Généralement, après la vérification effectuée à l'aide des tests. L'équipe de l'institut s'assure de la qualité du logiciel et du degré d'aboutie des objectifs.

III.1.5. Livraison

Durant cette étape nous livrons le produit au service informatique du HCEFLCD pour qu'il puisse l'utiliser et l'exploiter à sa guise.

III.1.6. Maintenance

Cette étape consiste à modifier le logiciel après sa livraison. Elle comprend toutes les actions correctives « maintenance corrective » ainsi que les actions évolutives « maintenance évolutive » qu'exige l'application.

Pour élaborer notre projet, nous avons adopté le cycle de vie suivant :

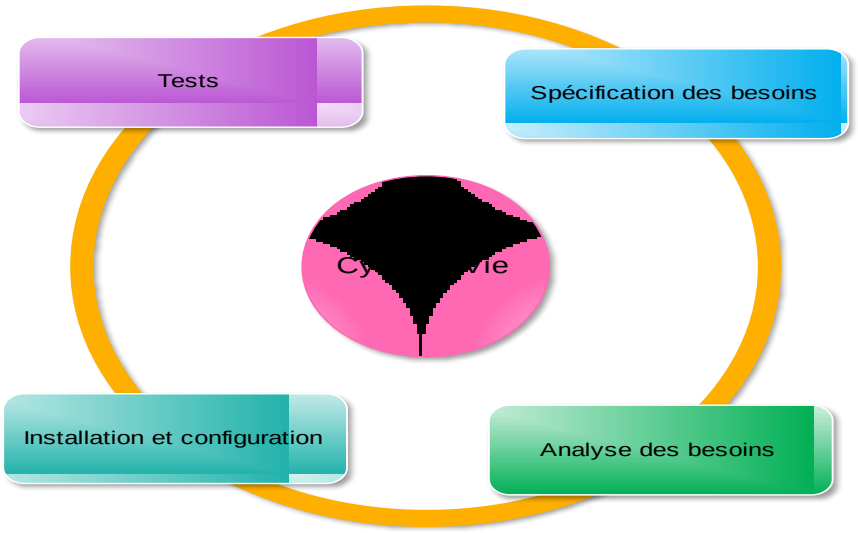

Figure n° 3: Cycle de vie

III.2. Product BreakDown Structure(PBS)

Le Product Breakdown Structure (PBS) répond à quoi ? C'est la décomposition arborescente du produit en éléments.

Pour découper notre projet en éléments, nous allons adopter la hiérarchie suivante :

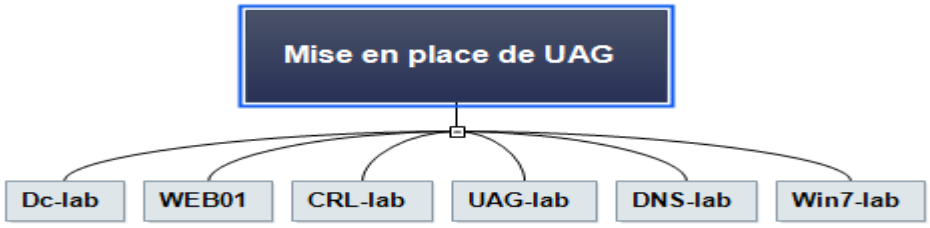

Figure n° 4: Product Breakdown Structure (PBS)

III.3. Work BreakDown Structure (WBS)

Work BreakDown Structure (WBS) est une méthode de découpage hiérarchique arborescente du projet en composants élémentaires.

Ci-après le découpage hiérarchique de notre projet : la mise en place d'un serveur UAG.

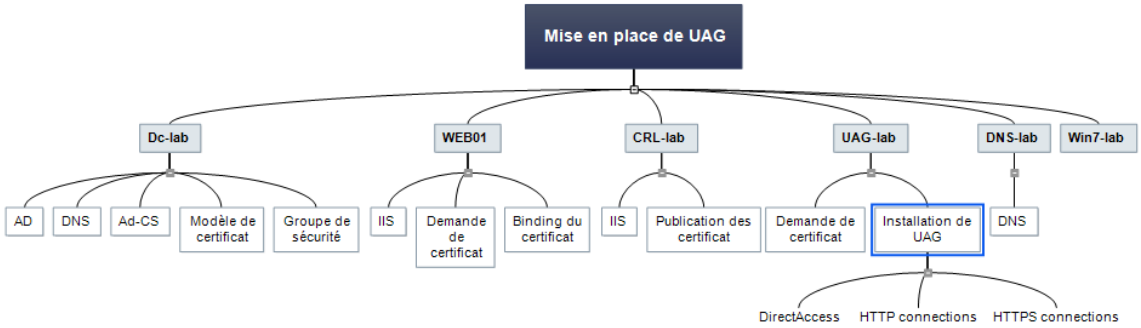

Figure n° 5: Work Breakdown Structure (WBS)

III.4. Digramme de GANTT

Durant notre période de stage, nous avons eu le souci d'assurer la réalisation de notre projet, c'est pourquoi nous avons adopté une planification qui s'illustre par le diagramme de GANTT .Ce diagramme est un outil permettant de modéliser la planification des tâches nécessaires à la réalisation d'un projet.

Le diagramme de Gantt suivant présente les différentes itérations de notre projet avec leur taux de finalisation.

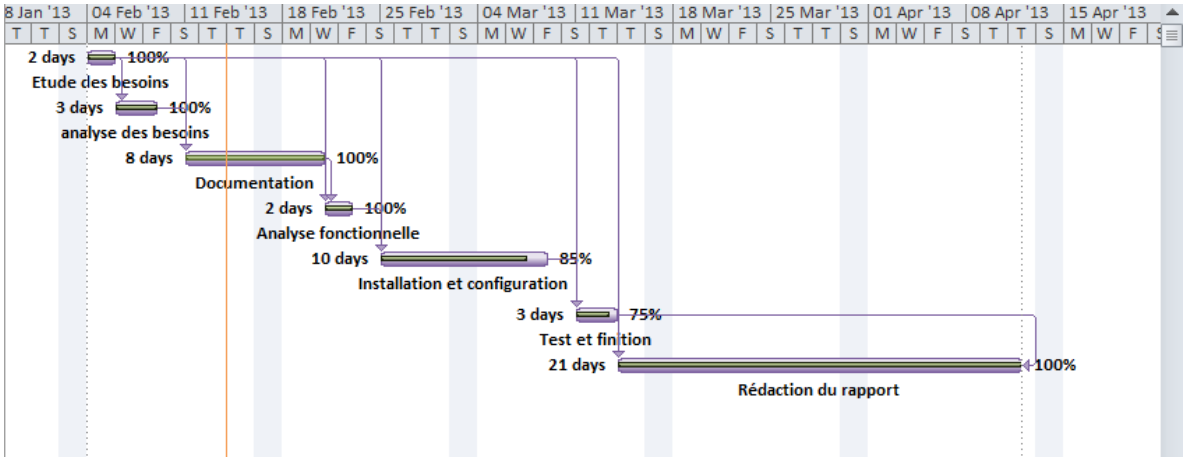

Figure n° 6: Diagramme de GANTT

Chapitre II

Microsoft Forfront Unified Acces Gateway et Direct Access

I. Microsoft Forefront Unified Access Gateway (UAG)

Avant d'entamer notre projet consistant à mettre en place un serveur UAG qui est un pare-feu et une passerelle d'accès aux applications, il semble pertinent de commencer par préciser qu'est-ce qu'un serveur UAG et de définir quel rôle peut-il jouer dans l'amélioration du HCEFLCD.

I.1. Historique

Historiquement, le premier produit de la gamme Forefront produit chez Microsoft, était Microsoft Internet Security and Acceleration Server 2006, le pare-feu de Microsoft intégrant des fonctionnalités de filtrage avancés aussi bien au niveau réseau qu'applicatif.

C'est en 2006 que Microsoft a racheté la société Whales Communications et son produit « Intelligent Application Gateway and Application Optimizers ». Ce produit se caractérise par le fait d'embarquer ISA Server 2004 pour ses fonctions de pare-feu avancés ainsi que pour se protéger lui-même, rien de plus. Fin 2009, Microsoft a mis à disposition le successeur d'ISA Server : Forefront Threat Management Gateway 2010.

Tout naturellement, Microsoft se devait de proposer une nouvelle version d'IAG. Ce fut chose faîte fin 2009 avec Forefront Unified Access Gateway 2010, réutilisant Forefront TMG 2010 pour se protéger.

I.2. Présentation de Forefront UAG

Forefront Unified Access Gateway assure un accès sécurisé aux ressources de l'entreprise quel que soit leur emplacement ou les terminaux utilisés, y compris les PC et appareils mobiles, gérés ou non, fortement inspiré de Microsoft Intelligent Application

Gateway, Forefront UAG combine diverses options de connectivité du VPN SSL au Windows DirectAccess avec des configurations et des stratégies prédéfinies de protection. Ainsi, Forefront UAG simplifie et centralise l'administration pour en réduire les coûts.

Forefront UAG est un produit un peu différent des autres chez Microsoft car il se positionne sur plusieurs tableaux :

- La publication de ressources de l'entreprise à l'extérieur ;
- La sécurisation des accès aux ressources internes de l'entreprise.

Forefront UAG s'appuie sur une connaissance approfondie des applications publiées, une analyse de l'état des appareils utilisés pour y accéder et l'identification de l'utilisateur, pour assurer un contrôle d'accès fin et précis. De plus, Forefront UAG, il est évolutif. Si une méthode d'authentification n'existe pas, rien ne nous empêche de la développer. UAG bénéficie donc d'une souplesse remarquable.

Une des plus grandes améliorations dont bénéficie Microsoft Forefront UAG en comparaison avec Forefront TMG est la capacité de fournir un portail Web pour les utilisateurs de l'Internet qui ont besoin d'accéder aux applications internes.

Forefront UAG utilise une terminologie appelé « trunk Portal ». Un tronc est une combinaison d'une adresse IP, le port HTTP / HTTP et un certificat quand un tronc HTTPS doit être créé. Le tronc portail est le point d'entrée pour toutes les applications publiées dans ce portail. Il est possible de s'authentifier sur ce portail en utilisant différents services d'annuaires comme Active Directory, Netscape et plus encore. Un tronc portail permet également à l'administrateur de Forefront d'appliquer les politiques d'accès Endpoint UAG. Une politique d'accès Endpoint est en mesure de vérifier l'état de conformité du client. Par exemple, le client doit avoir le Pare-feu Windows activé, toutes les mises à jour Windows doivent être installées sur la machine et la machine doit être joint au domaine Active Directory interne.

I.2.1. Accès en tout lieu

Quel que soit l'emplacement des utilisateurs ou des terminaux utilisés, Forefront UAG sert de passerelle consolidée via un portail unique.

Forefront UAG Simplifie et sécurise l'accès à distance, il prend en charge une vaste gamme d'applications Microsoft (Microsoft SharePoint®, Microsoft Exchange Server, Remote Desktop Services et Microsoft Dynamics® CRM) via des modules d'optimisation prédéfinis. Ces modules analysent le comportement des applications, des interactions navigateur-serveur et des exigences de l'appareil utilisé pour créer des paramètres optimaux et des règles de sécurité spécifiques.

De plus, UAG met DirectAccess à la portée des applications et des ressources exécutées sur l'infrastructure existante, il prend en charge les postes clients de version antérieure ou non-Windows via un VPN SSL ou une autre connexion.

I.2.2. Sécurité intégrée

Afin d'améliorer la sécurité et de renforcer la conformité de l'entreprise, Forefront UAG limite l'exposition avec des contrôles d'accès fins, permet d'une part, une analyse détaillée de l'état des terminaux et des autorisations de l'utilisateur. D'autre part, il permet aux administrateurs d'élaborer des règles précisant les conditions que les postes clients doivent remplir à chaque transaction.

I.2.3. Administration simplifiée

Forefront UAG Offre plus de souplesse en proposant plusieurs types d'équipements dont des appliances matérielles, des appliance virtuelles ou des logiciels serveurs. Il facilite le regroupement de plusieurs serveurs Forefront UAG en une grille dont tous les membres partagent la même configuration et qui sont gérés comme une seule entité. Il utilise aussi des assistants pour simplifier le déploiement initial et les tâches courantes. Et il s'intègre à Microsoft SQL Server et à System Center Operations Manager pour simplifier respectivement la journalisation et l'administration.

II. Forefront UAG et DirectAccess

Forefront Unified Access Gateway (UAG) DirectAccess supporte les dernières innovations de Microsoft dans le domaine de mobilité, en particulier il intègre le DirectAccess. Forefront UAG DirectAccess permet aux utilisateurs distants avec l'expérience d'une connexion transparente au réseau interne en tout moment d'avoir accès à

Internet. Lorsque Forefront UAG DirectAccess est activé, les demandes de ressources réseau interne (telles que les serveurs de courrier électronique, les dossiers partagés, les serveurs de gestion, ou les sites Web intranet) sont bien dirigées vers le réseau interne, sans avoir besoin de se connecter à un VPN.

II.1. C'est quoi DirectAccess ?

DirectAccess permet de se connecter à distance au réseau de son entreprise. Cependant, cela diffère d'une connexion VPN puisqu'il n'y a pas besoin d'établir une connexion dans le gestionnaire de connexion. Une fois connecté, l'utilisateur accède au réseau comme s'il était à son entreprise.

Grâce à DirectAccess, il est possible de manager facilement le parc d'ordinateurs d'une entreprise puisque les mises à jour des GPO ou les mises à jour software par exemple, se feront indépendamment de la connexion ou non d'un utilisateur. L'ordinateur client est donc constamment à jour avec les normes de sécurité de l'entreprise. L'interconnexion entre les postes se fait donc de façon bilatéral.

IPsec et IPv6 qui sont utilisés pour DirectAccess permettent notamment une encryption des données en utilisant différents algorithmes comme AES ou 3DES. Ainsi les communications restent protégées. Mais il est aussi possible de décider à quelles applications ou quels serveurs auront accès les utilisateurs.

II.2. Le puzzle DirectAccess

DirectAccess est un sujet à la fois simple et complexe. C'est simple car ce n'est que l'assemblage de technologies existantes, c'est complexe car il faut en maîtriser l'assemblage. Nous sommes donc en face d'un puzzle qui, une fois assemblé, donne entière satisfaction. Passons en revue les pièces qui le composent :

- **IPv6 :** DirectAccess est basé nativement sur le couple IPv6 / IPsec. Bien évidemment, la technologie IPv4 étant encore massivement répandue et IPv6 n'étant pas près de la remplacer avant plusieurs années, des technologies ont été mises au point afin d'encapsuler des paquets IPv6 dans des paquets IPv4 ;
  En fonction du type de réseau il est préférable d'utiliser certaines technologies :

Scénario	*Protocole*	*Technologie*
Adressage IPv6 sur le réseau Interne de l'entreprise reposant sur IPv4	**ISATAP**	Encapsule le trafic IPV6 dans des trames IPv4
Poste de travail avec connectivité internet publique	**6to4**	Encapsule le trafic IPV6 dans des trames IPV4
Poste de travail avec connectivité Internet assurée par un mécanisme de translation (NAT)	**Teredo**	Encapsule le trafic IPV6 dans le protocole UDP
Poste de travail disposant d'une connectivité Internet limitée à HTTPS	**IP-HTTPS**	Encapsule le trafic IPV6 dans le protocole HTTPS
Résolution de noms DNS interne	**DNS64/NAT64**	Assure la résolution des noms DNS internes et met en place une translation pour les systèmes non compatibles avec IPV6

Tableau n° 2: technologies de transition vers IPv6

- **IPSec :** la sécurisation des flux de données échangées entre un client en situation de mobilité et le réseau interne de l'entreprise repose sur des tunnels IPSEC. On distinguera plusieurs types de tunnels IPSEC :

  - Tunnel d'infrastructure : Ce premier tunnel est initialisé par le système d'exploitation entre le client DirectAccess et le serveur Microsoft Forefront Unified Access Gateway. L'authentification de ce tunnel repose sur le certificat « ordinateur » ainsi que sur une authentification. Ce tunnel est limité au système d'exploitation pour lui permettre d'accéder à des ressources d'infrastructure (DNS, Antivirus, …) et d'administrer le poste de travail ;

  - Tunnel utilisateur : Ce second tunnel est initialisé par l'utilisateur quand il tente d'accéder à une ressource de l'entreprise. Il est initialisé entre le client DirectAccess et le serveur Microsoft ForeFront Unified Access Gateway. L'authentification de ce tunnel repose sur le certificat « ordinateur » ainsi que sur l'authentification. Ce tunnel est dédié à

l'utilisateur pour accéder aux ressources internes de l'entreprise. Il est possible de mettre en œuvre une authentification forte à ce niveau ;

- Tunnel application : Ce dernier type de tunnel est optionnel. Il permet de configurer un groupe de serveurs de l'entreprise pour établir un tunnel IPSEC qui se terminera sur ces serveurs. L'intérêt de cette démarche est de pouvoir exiger d'appliquer de nouveaux critères pour l'authentification (utilisateur ou ordinateur appartenant à un groupe donné, authentification carte à puce obligatoire, exigence de conformité du poste de travail, …).

- **Pare-Feu personnel :** Depuis Windows Vista, le pare-feu personnel du système d'exploitation intègre la prise en charge d'IPSEC. Pour cette raison, il est nécessaire de conserver un pare-feu sur le poste de travail. Côté client, celui du système d'exploitation peut être conservé, Côté serveur, c'est la même chose. nous conservons le pare-feu personnel de Windows Server 2008 R2 ;

- **Systèmes d'exploitation :** côté client seules les éditions Entreprise et Ultimate de Windows 7 sont éligibles à DirectAccess, ces systèmes sont nécessairement membre d'un domaine. Côté serveur, les seuls systèmes d'exploitation supportés sont Windows Server 2008 R2 standard et ultérieurs;

- **Name Resolution Policy Table :** comment s'effectue la résolution de noms DNS? La résolution des noms DNS interne repose : côté client, sur la «Name Resolution Policy Table ». La configuration mise en place dans la NRPT indique que la résolution des noms DNS est assurée par un hôte IPv6 qui est en fait le serveur UAG. DNS64/NAT64 récupère alors les demandes de résolution de noms DNS et assure le traitement de la manière suivante :

  - Demande de résolution du nom DNS en IPv6 et IPv4 ;
  - Si la réponse retournée est directement en IPv6 alors l'information retourne au client ;
  - Si la réponse est uniquement IPv4 dans ce cas l'information est transmise à NAT64 ;

- NAT64 va par la suite générer une adresse IPv6 temporaire et assurer la correspondance avec l'adresse IPv4;
- Finalement, l'information IPv6 est retournée au client.

- **Network Location Server :** est un serveur Web qui va héberger une URL de localisation accessible via HTTPS seulement depuis l'intranet de l'entreprise. Il montrera que nous avons accès au réseau interne ;

- **Forefront Unified Access Gateway :** Certes, il est possible de faire du DirectAccess sans UAG, mais l'utilisation de ce dernier sera plus avantageuse D'abord, vu sa capacité d'assurer la haute disponibilité. Ensuite, parce qu'il permet la répartition de charge matérielle ou logicielle au sein de la ferme UAG. Et enfin, parce qu'il propose également un portail d'applications publiées avec prise en charge du SSO, etc.

- **DirectAccess Connectivity Wizard :** est un composant optionnel mais tellement nécessaire pour l'utilisateur final. DirectAccess est tellement transparent pour l'utilisateur au point qu'il ne sait pas si cela fonctionne ou non. Pour régler cet problème, Microsoft a mis à disposition avec le Microsoft ForeFront Unified Access Gateway une version du « DirectAccess Connectivity Wizard » ;

- **Network Access Protection :** Composant optionnel, servant à encourager la mise en conformité des ordinateurs aux spécifications de sécurité et d'intégrité, et sert aussi à réduire le risque de dissémination des programmes malveillants. Les ordinateurs non conformes peuvent être interdits d'accès aux ressources intranet ou de communication avec les ordinateurs conformes ;

- **Authentification double facteur :** Plus personne ne propose de solution de nomadisme sans prise en charge d'un ou de plusieurs moyens d'authentification à double facteur (ce que je détiens et ce que je sais voire qui je suis). DirectAccess n'échappe pas à cette règle. Avec Microsoft ForeFront Unified Access Gateway 2010, les possibilités ont été accrues. L'authentification du tunnel IPSEC « utilisateur » peut désormais exploiter :

- Une authentification par carte à puce ;
- Un mécanisme d'authentification de type « One Time Password » (OTP).

Ci-après le montage du puzzle pour un meilleur fonctionnement :

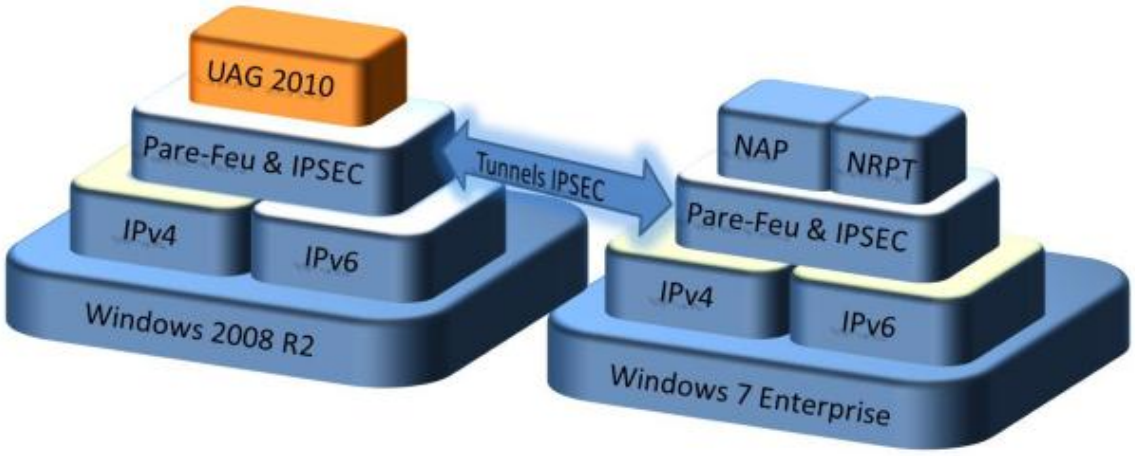

Figure n° 7: Le puzzle DirectAcceess

II.3. Les avantages du déploiement DirectAccess et Forefront UAG Ensemble

Lorsque Windows DirectAccess et Forefront UAG sont déployées ensemble, elles offrent une solution de sécurité d'accès améliorée et unifiée à travers ainsi que au-delà de l'environnement de l'entreprise. La valeur combinée de ces deux technologies permet aux services informatiques de fournir une meilleure productivité de l'utilisateur en établissant un équilibre entre l'exposition des ressources d'entreprise vers le monde extérieur et permet aussi de maintenir la sécurité et la conformité réglementaire. Forefront UAG s'allie à DirectAccess pour :

- Etendre ces bénéfices aux systèmes de version antérieure ou non-Windows via un VPN SSL et d'autres types de connexion ;
- Limiter les risques liés à la connexion de systèmes non gérés, de version

antérieure ou non-Windows, à l'aide de contrôles d'accès très fins ;

- Protéger la passerelle DirectAccess avec une solution Edge renforcée et un pare-feu intégré ;
- Simplifier le déploiement avec des assistants et des outils intégrés ;
- Assurer la montée en charge et l'administration à l'aide de groupes de serveurs et d'un équilibrage de la charge.

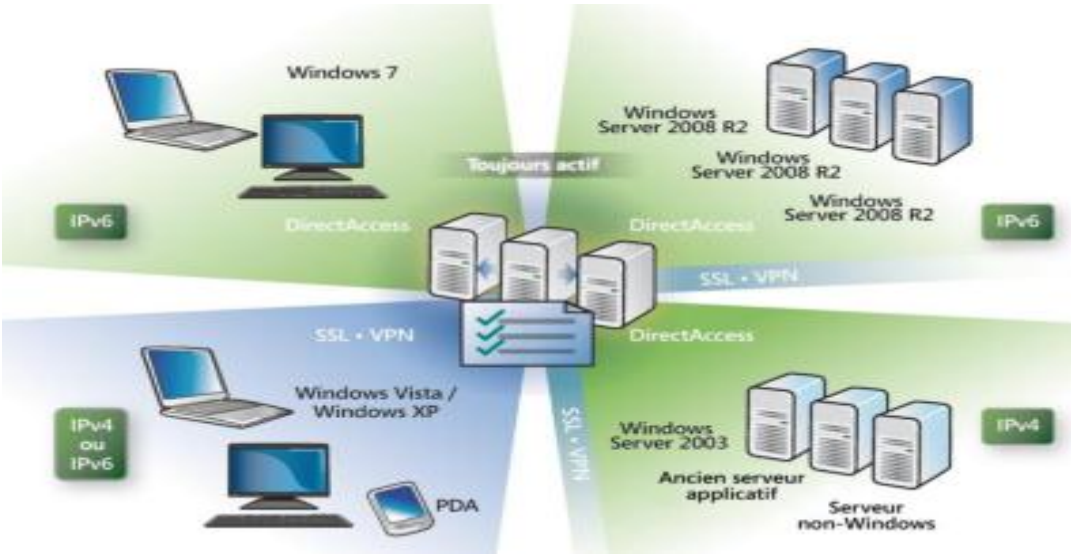

Figure n° 8: Forefront UAG et DirectAccess

Chapitre III

Mise en place du serveur UAG

I. Prérequis

Les exigences matérielles, du système et logiciels, requises pour l'installation et le déploiement Forefront Unified Access Gateway (UAG) sont les suivants :

I.1. Prérequis matériel

- Processeur : 2,66 gigahertz (GHz) ou processeur plus rapide. CPU dual core ;
- Mémoire : 4 Go ;
- Disque dur : 2,5 gigaoctet (Go) (en plus des exigences de Windows).
- Cartes réseau : Deux cartes réseaux qui sont compatibles avec le système d'exploitation de l'ordinateur. Ces cartes réseaux sont utilisées pour la communication avec le réseau interne de l'entreprise, et le réseau externe (Internet).

I.2. Prérequis logiciel

- Système d'exploitation : Forefront UAG peut être installé sur les ordinateurs exécutant le serveur standard Windows 2008 R2 ou Windows Server 2008 R2 Enterprise, systèmes d'exploitation 64 bits.

II. Environnement de mise en place

II.1. Environnement Matériel

Nous avons mis en place notre plateforme sur une lame de processeur **Intel Xeon E5540 @ 2,53** (**16 CPUs**), de disque dur de **300** Go et une RAM de **14** Go, de l'infrastructure de HCEFLCD basée sur HP BladeSystem de modèle Proliant BL460c G6.

II.2. Environnement Logiciel

- Système d'exploitation : Windows Server 2008 R2 X64 ;
- Rôle : HyperV qui est un système de virtualisation.

III. Architecture

L'architecture de la plateforme Forefront UAG et DirectAccess est la suivante :

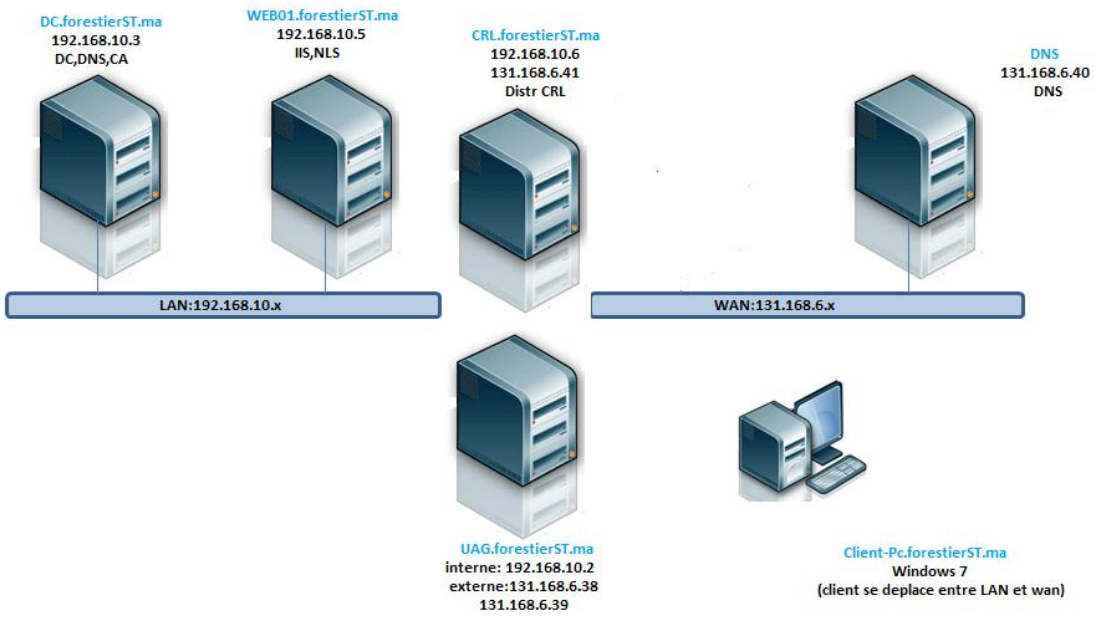

Figure n° 9: Plateforme Forefront UAG et DirectAccess

III.1. Descriptif de l'architecture

- La machine virtuelle DC : joue le rôle du contrôleur du domaine

  - Installation du système Windows server 2008 R2 ;
  - Changement du nom de machine
  - Mise à jour du système et Activation
  - Paramétrage IPv4 (192.168.10.3)
  - Paramétrage IPv6 : la machine est en ISATAP
  - Ajout du Rôle AD Domain Services
  - DCPROMO : création du domaine forestierST.ma ;
  - création reverse zone DNS ;

- Installation du Rôle AD CA ;
- Création d'un modèle de certificat DirectAccess IPsec EndPoint ;
- Création d'un modèle de certificat DirectAccess IPsec Tunnel ;
- Création d'un modèle de certificat Web Server exportable ;
- Modification de la GPO Default Domain Policy avec des règles autorisant sur le Pare-feu Windows : Echo Request ICMPv4 et v6 ;
- Config du DNS pour supprimer le nom ISATAP de la default global blocklist ;
- Config des CRLs ;
- Modification de la GPO default domain policy pour auto enrollment des certificats ordinateurs ;
- Création d'un groupe de sécurité DA_Clients dans l'Active Directory (Client-PC est membre de ce groupe) ;
- Création d'un groupe de sécurité DA_Servers dans l'Active Directory (UAG est membre de ce groupe).

- **La machine virtuelle WEB01 : joue le rôle de NLS**

  - Installation du système Windows server 2008 R2 ;
  - Changement du nom de machine ;
  - Mise à jour du système et activation ;
  - Paramétrage IPv4 (192.168.10.5) ;
  - Paramétrage IPv6 : la machine est en ISATAP
  - Ajout dans le domaine forestierST.ma ;
  - Demande de certificat de type Web Server exportable ;
  - Installation du rôle Web Server ;
  - Binding du certif SSL sur le site web par défaut.

- **La machine virtuelle CRL: joue le rôle de serveur Web servant la liste des certificats révoqués**

  - Installation du système Windows server 2008 R2 ;
  - Changement du nom de machine ;
  - Mise à jour du système et activation ;
  - Paramétrage IPv4 (192.168.10.6) (131.168.6.41) ;

- Paramétrage IPv6 : la machine est en ISATAP ;
- Ajout dans le domaine ForestierST.ma ;
- Installation du rôle Web Server.

- **La machine virtuelle UAG: joue le rôle de serveur Forefront UAG et de passerelle DirectAccess**

  - Installation du système Windows server2008 R2 ;
  - Changement du nom de machine ;
  - Mise à jour du système et Activation ;
  - paramétrage IPv4 (192.168.10.2) (131.168.6.38) ;
  - paramétrage IPv6 : la machine est en ISATAP ;
  - Ajout dans le domaine ForestierST.ma ;
  - Demande de certificat complémentaire de type Web Server (pour IP-HTTPs) ;
  - Installation de Forefront UAG (nous allons expliquer les détails de cette installation ultérieurement).

- **La machine virtuelle DNS: joue le rôle de serveur DNS publique ainsi que de serveur Web publique**
  - Installation du système Windows server 2008 R2 ;
  - Changement du nom de machine ;
  - Mise à jour du système et Activation ;
  - paramétrage IPv4 (131.168.6.40).

- **La machine virtuelle, Client-Pc est un client Windows 7 Entreprise, configurée comme client DirectAccess**

  - Installation de WIN7DA
  - Ajout dans le domaine ForestierST.ma ;
  - Deux interfaces réseau (LAN, WAN)
    Adresse sur la carte WAN : 131.168.6.33
    Adresse sur le LAN : 192.168.10.4

IV. Installation et configuration du serveur Forefront UAG

Une fois toutes les machines installées, nous allons passer à la préparation de la machine UAG qui va exécuter Forefront Unified Access Gateway.

Lors de l'installation de Forefront UAG, vous devez disposer des autorisations d'administrateur sur le serveur local. Vous devez également, être un utilisateur du domaine auquel appartient le serveur Forefront UAG,

Quand toutes ces conditions sont remplies nous pouvons commencer le processus d'installation.

Figure n° 10: Installation de Forefront UAG

Durant l'installation, nous veillons à lire l'accord de licence d'utilisation et à le valider, puis, nous définissons l'emplacement d'installation de Forefront UAG. Alors que l'installateur s'occupe d'installer les rôles et les composantes nécessaires, ainsi qu'il installe Forefront TMG packagé spécialement pour UAG et qui joue le rôle de pare-feu réseau et protège la machine.

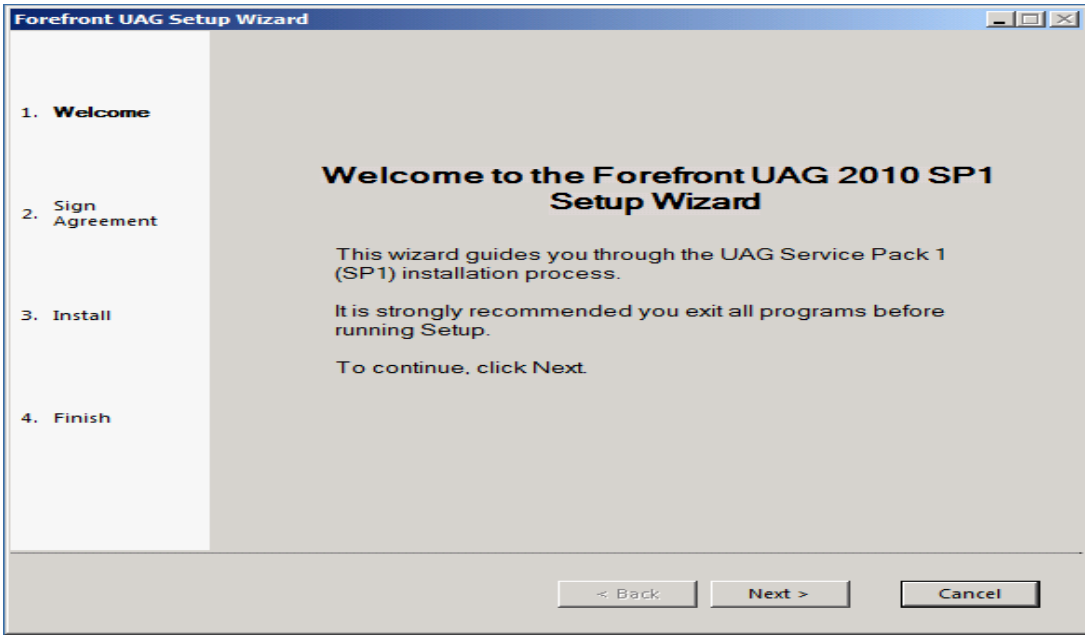

Figure n° 11: Installation avancée de Forefront UAG

Une fois, l'installation terminée il est nécessaire d'effectuer un redémarrage, Après le redémarrage, nous pouvons ouvrir la console d'administration de Forefront UAG.

L'assistant de configuration nous permet d'accéder à certains paramètres de configuration réseau de base comme les paramètres de la carte réseau et ceux de la topologie du serveur UAG.

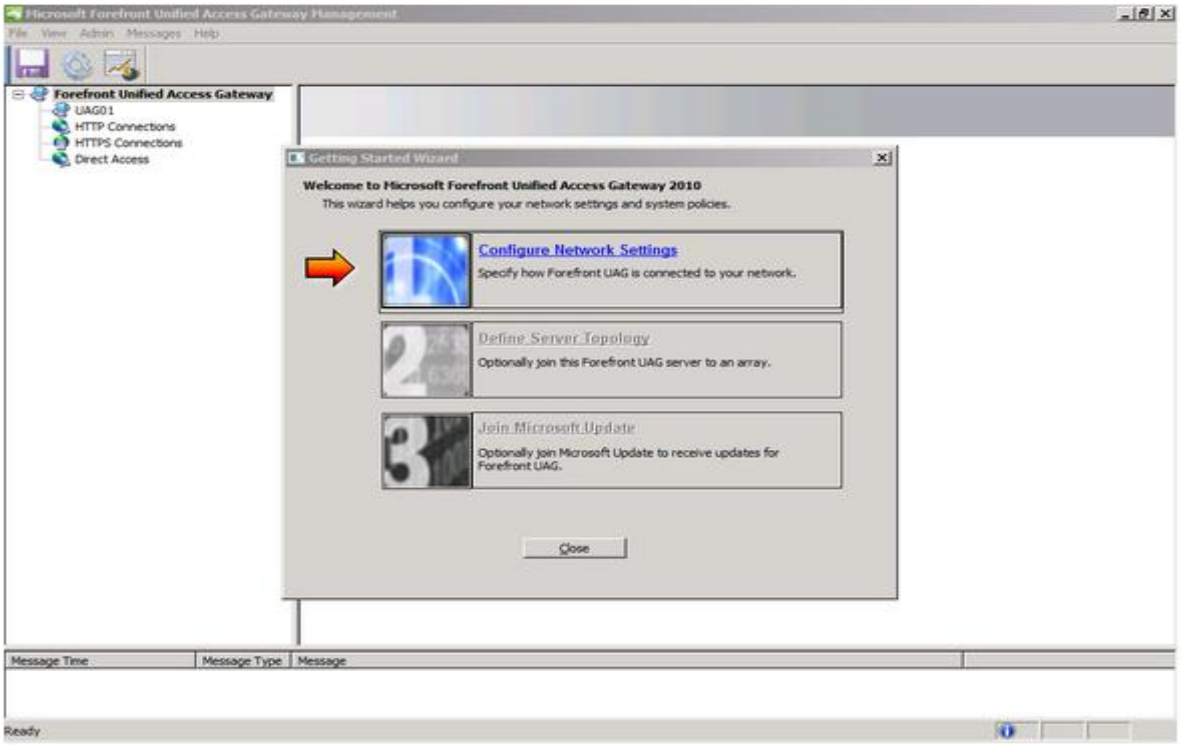

Figure n° 12 : Assistant de configuration

Définir les réglages des cartes réseaux est important pour informer l'UAG à la fois du type de la carte réseaux qui se connecte au réseau interne (confiance) et de celle qui se connecte au réseau externe (non fiable).

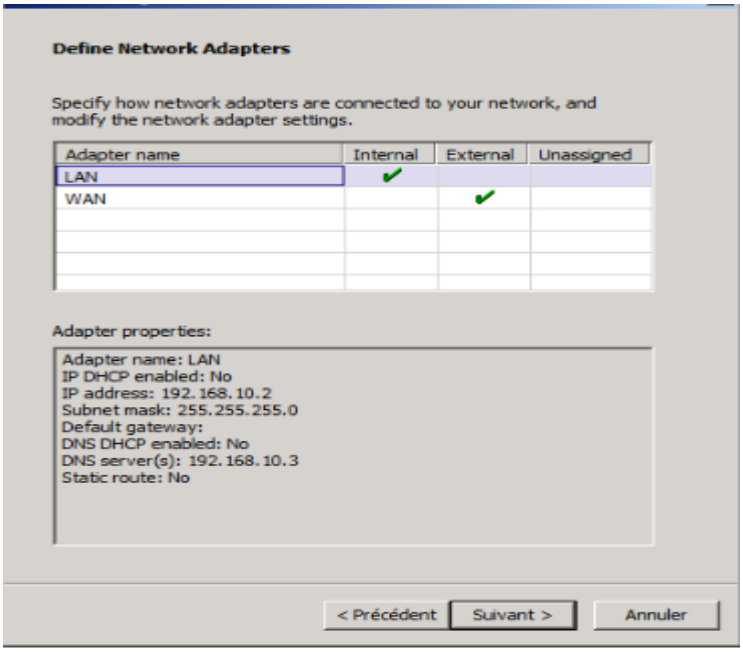

Figure n° 13: Définir les adaptateurs réseau

Ensuite nous allons choisir la topologie utilisée : ferme de serveurs UAG ou bien machine indépendante.

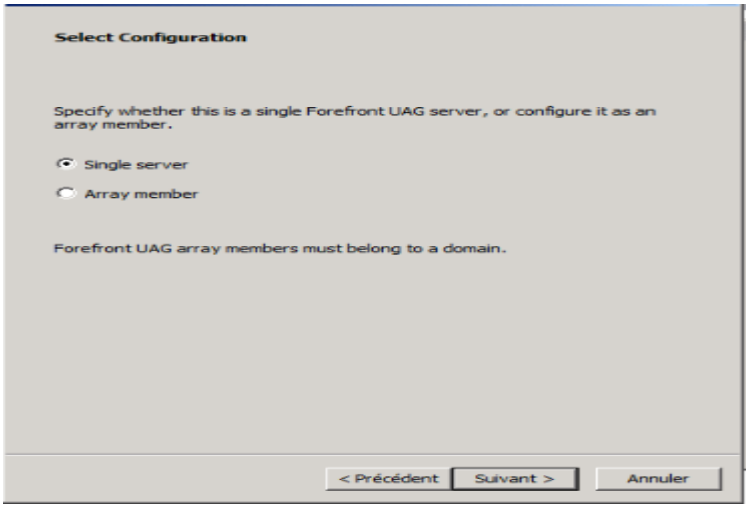

Figure n° 14 : Définir la topologie du serveur UAG

La dernière étape de configuration consiste à activer la mise à jour via Microsoft Update (si ce n'est pas déjà fait)

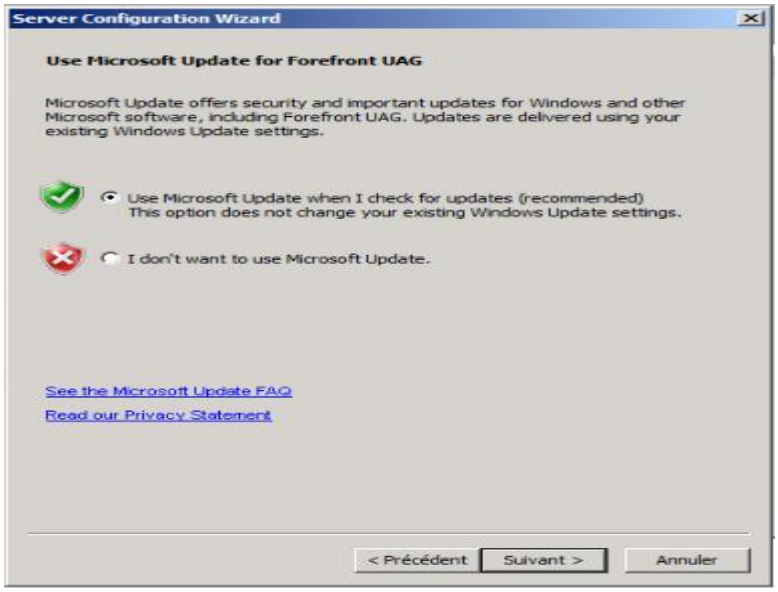

Figure n° 15 : Activation des mises à jour

Et voilà, l'installation est presque prête, il reste à activer la configuration (opération classique pour les administrateurs IAG/UAG).

Figure n° 16: Demande d'activation

Et là c'est réellement terminé, le serveur Forefront UAG est prêt à être configuré pour les accès distants (Portail, Passerelle Terminal Server, VPN, DirectAccess).

IV.1. Configuration de DirectAccess

Avant de commencer la configuration du DirectAccess, il faut s'assurer que toutes les conditions préalables ont été remplies. Sinon les étapes de l'assistant ne seront pas achevées convenablement.

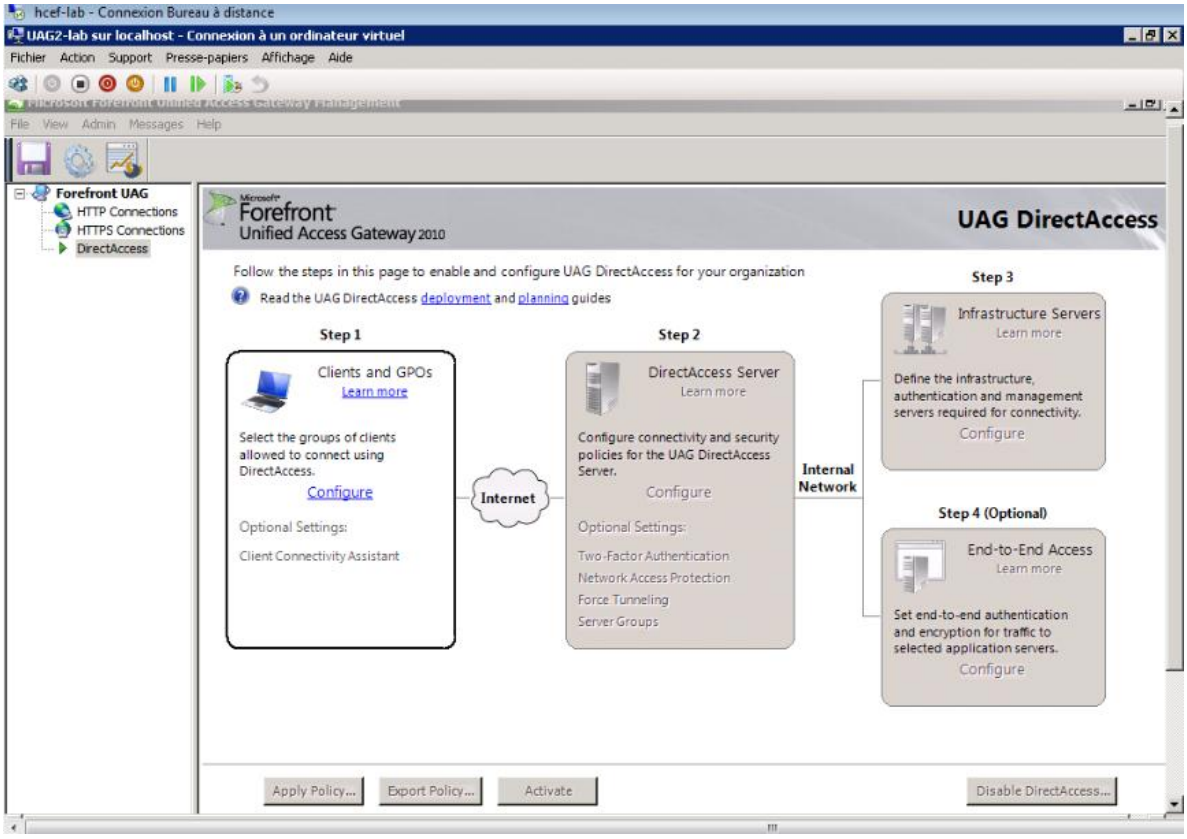

Figure n° 17 : Console DirectAccess dans Forefront UAG

Nous voulons permettre aux clients DirectAccess de se connecter aux ressources internes et nous souhaitons aussi lui permettre la gestion à distance des ordinateurs DirectAccess comme le montre la capture d'écran ci-dessous.

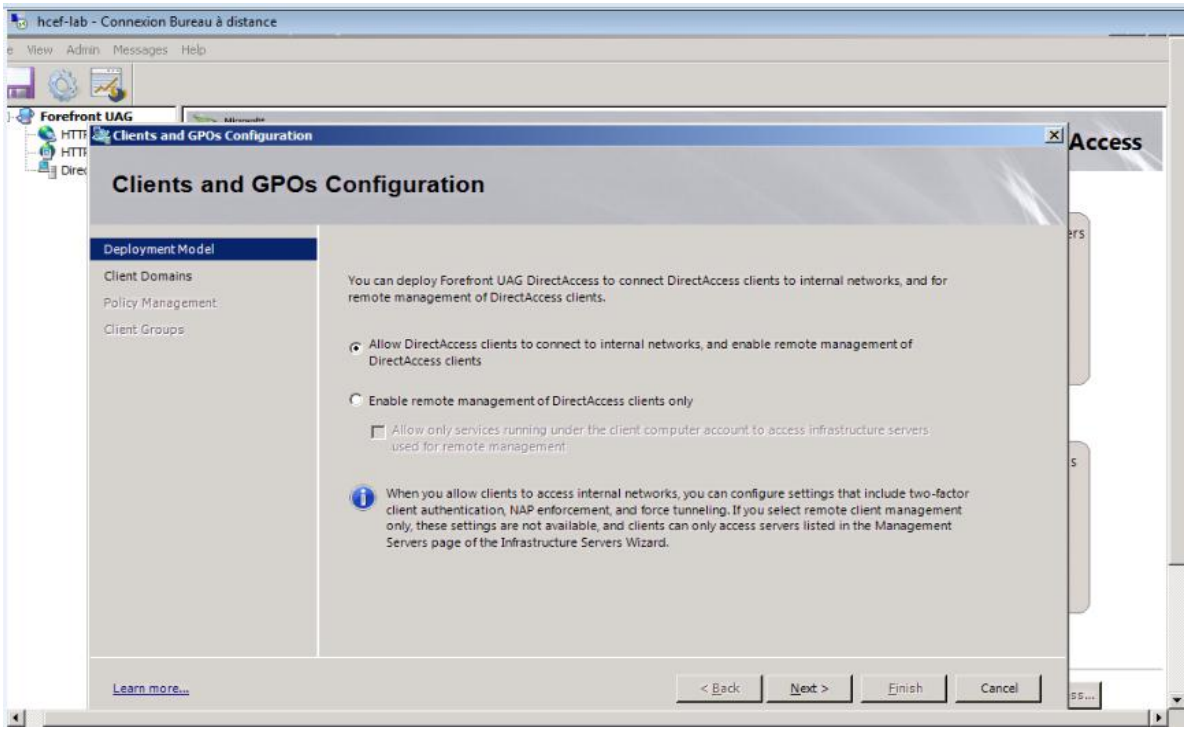

Figure n° 18 : Activer DirectAccess pour accéder aux ressources internes

Après avoir activé DirectAccess pour les ordinateurs clients de notre infrastructure Active Directory, maintenant nous devons sélectionner le domaine auquel nous désirons activer DirectAccess.

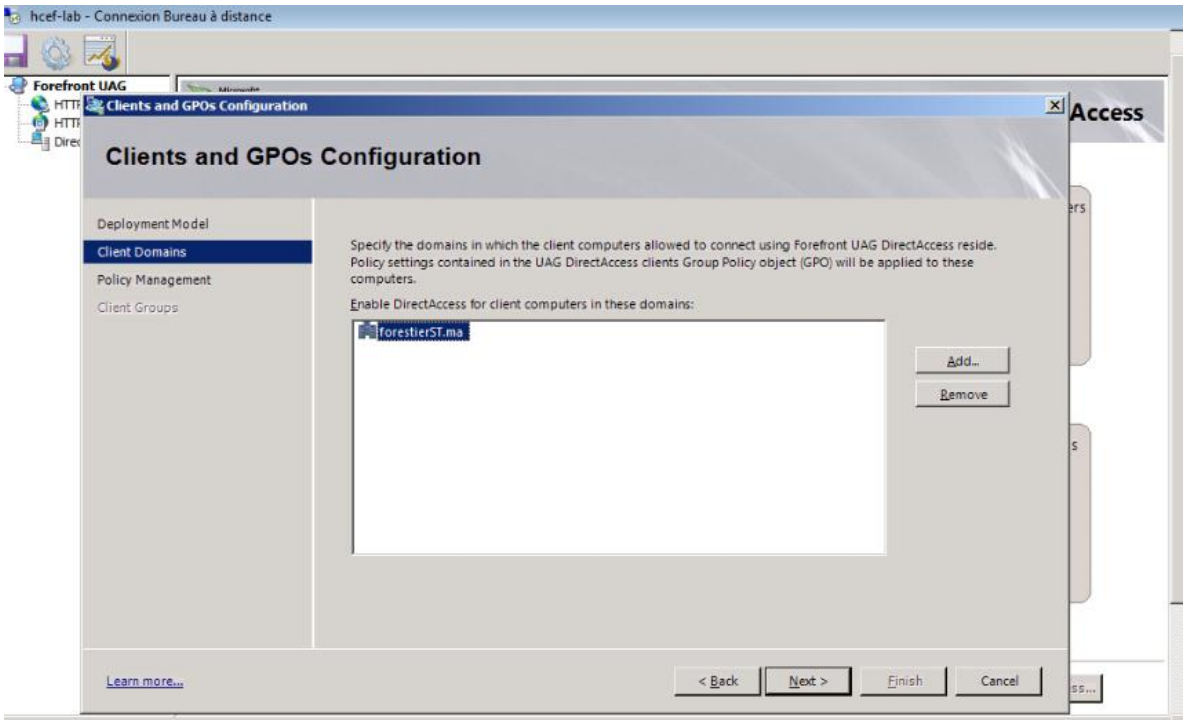

Figure n° 19 : Sélectionne du domaine Active Directory

Forefront UAG crée automatiquement trois objets de stratégie de groupe qui seront liés plus tard au plus haut niveau du domaine Active Directory et filtrés par filtrage de sécurité de stratégie de groupe. Les administrateurs sont en mesure de modifier les paramètres par défaut.

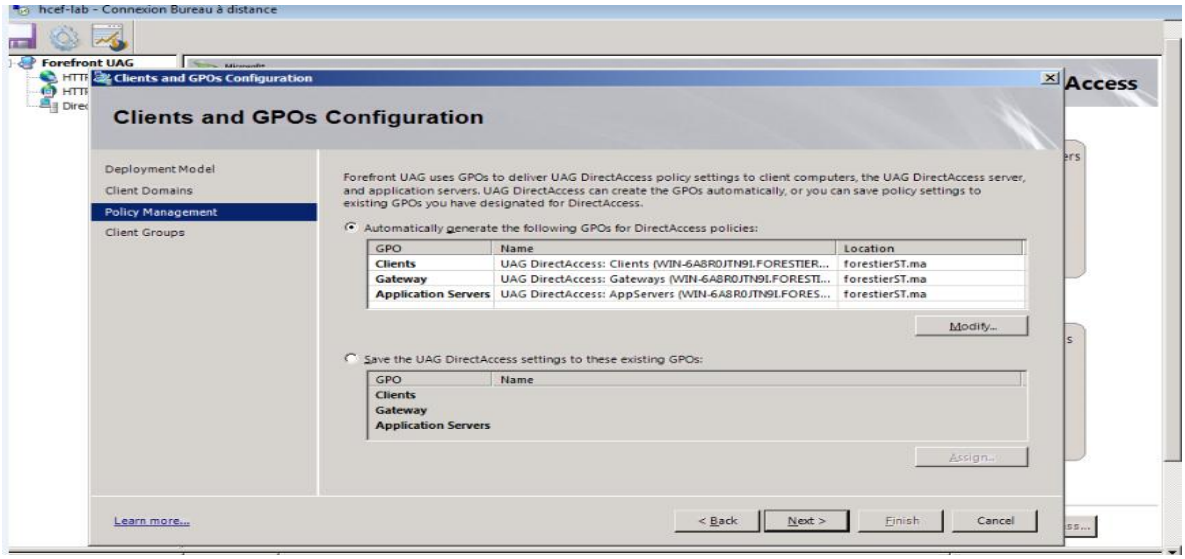

Figure n° 20 : Création automatiquement des objets de stratégie de groupe

Il est possible d'activer DirectAccess pour un groupe de sécurité Active Directory ou pour les unités d'organisation (UO).

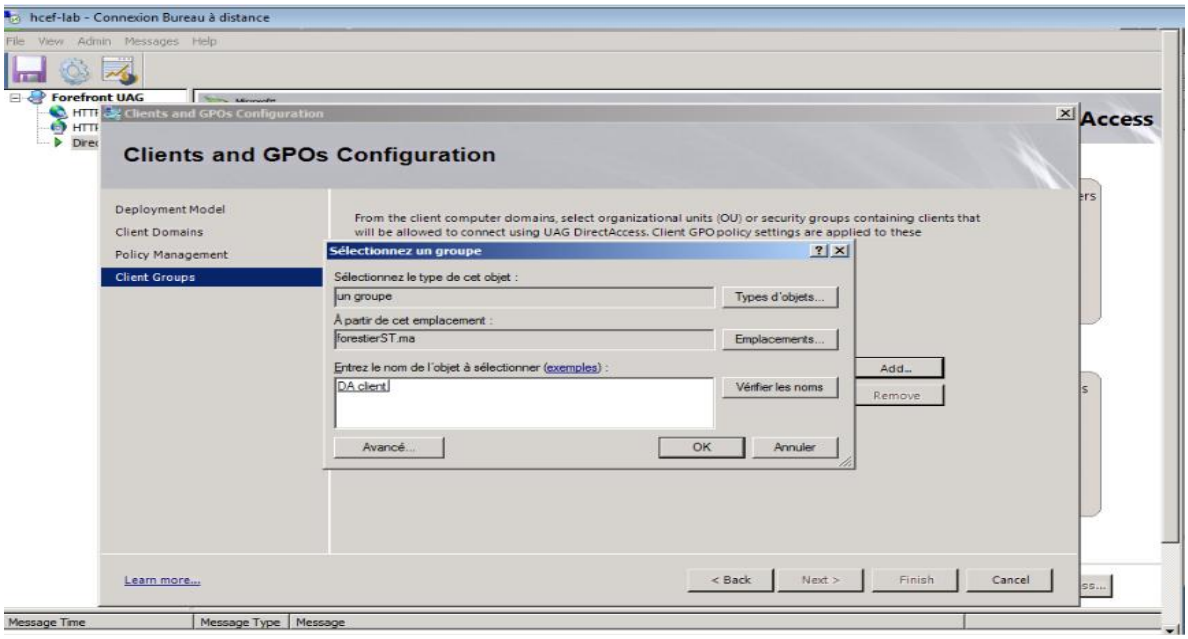

Figure n° 21: Activer DirectAccess pour groupe

Maintenant nous allons activer l'assistant de Connectivité de Client, qui constitue une aide visuelle pour l'utilisateur connecté en DirectAccess.

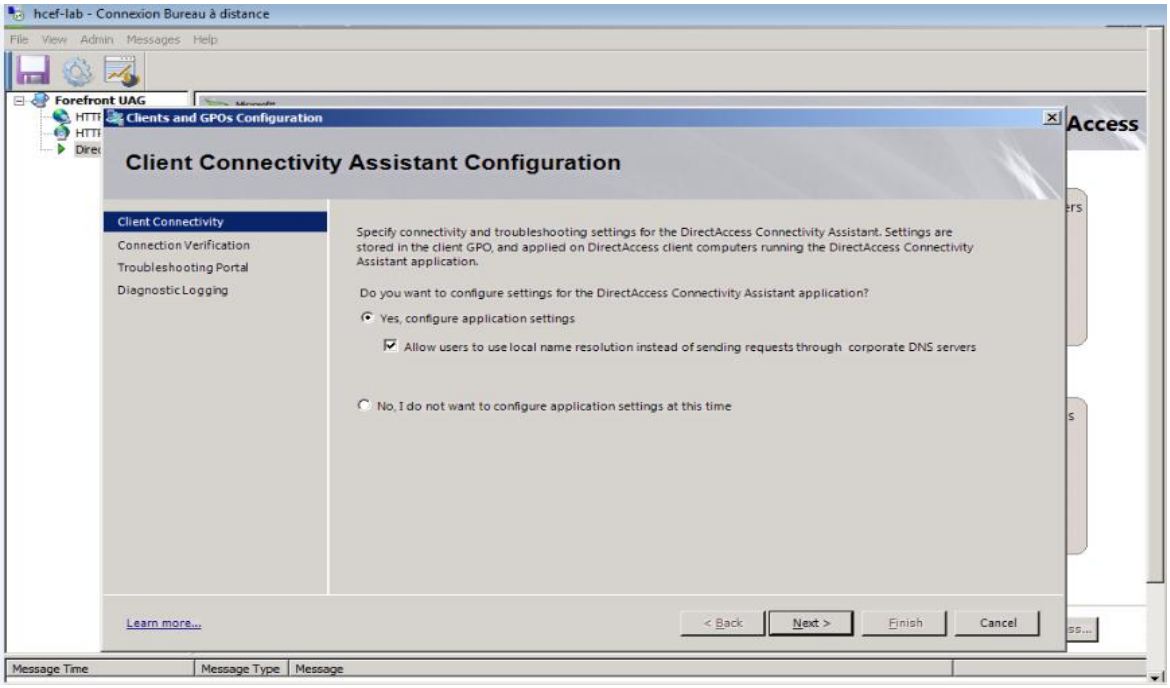

Figure n° 22 : Assistant de configuration du client connectivité

Il est possible de définir des vérificateurs de connectivité qui permettent de savoir si le client DirectAccess dispose d'un accès aux ressources hébergées dans le système d'information.

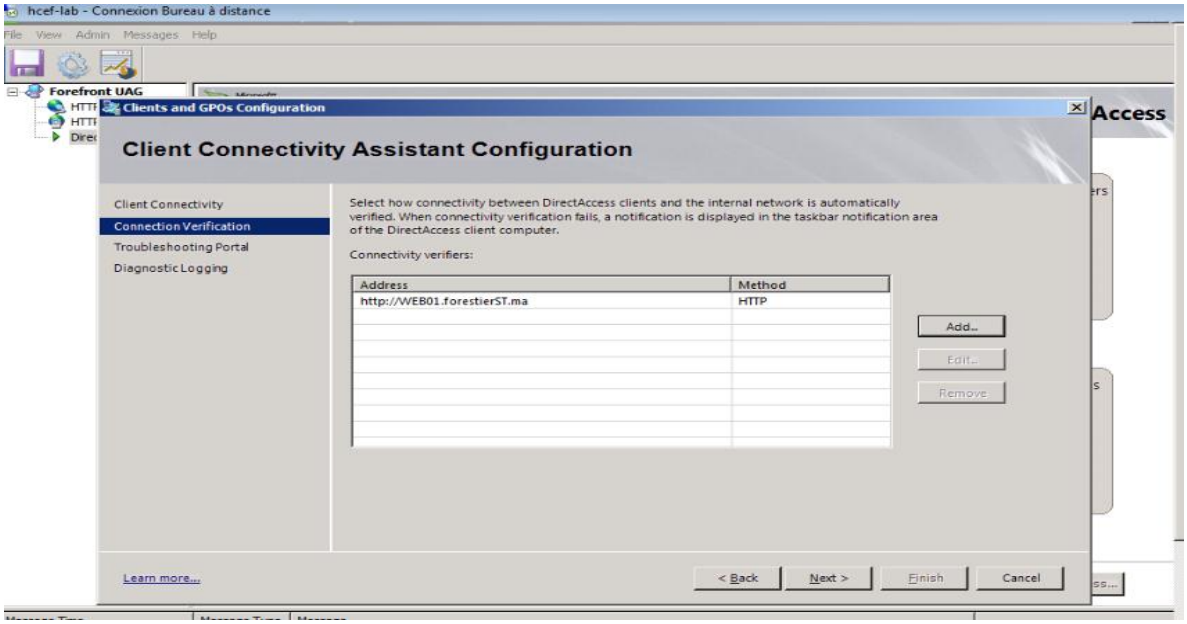

Figure n° 23: Vérification du client connectivité

Forefront UAG DirectAccess nécessite deux Internet conducteur face adresses IPv4. Et en ce qui concerne l'adresse IP interne du serveur Forefront UAG nous devons créer un enregistrement d'hôte avec le nom ISATAP dans le DNS interne zone de recherche directe de notre infrastructure Active Directory.

Nous avons pris en considération toutes ces mesures et conditions comme nous avons également supprimé ISATAP de la liste des blocs de requête : DNS mondial. Pour pouvoir accéder aux éléments de paramétrage du serveur DirectAcces.

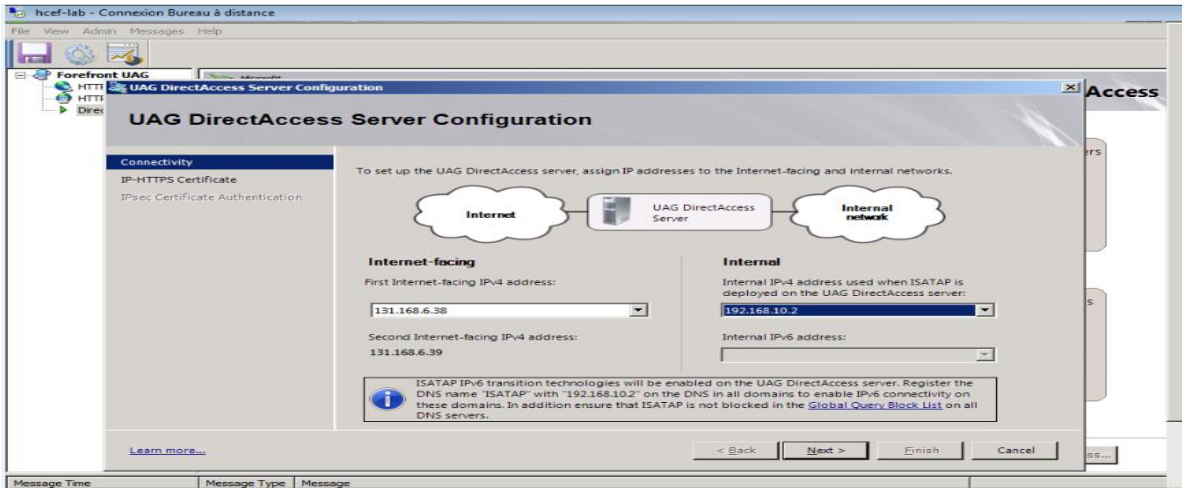

Figure n° 24: Configuration des adresses IP

L'étape suivante consiste à sélectionner le certificat de serveur utilisé pour authentifier les clients DirectAccess. Le certificat en question est utilisé pour IP-HTTPS. Il s'agit de la dernière technologie de transition utilisée par un client DirectAccess lorsque la connectivité IPv6 native ou une connexion Teredo n'est pas possible.

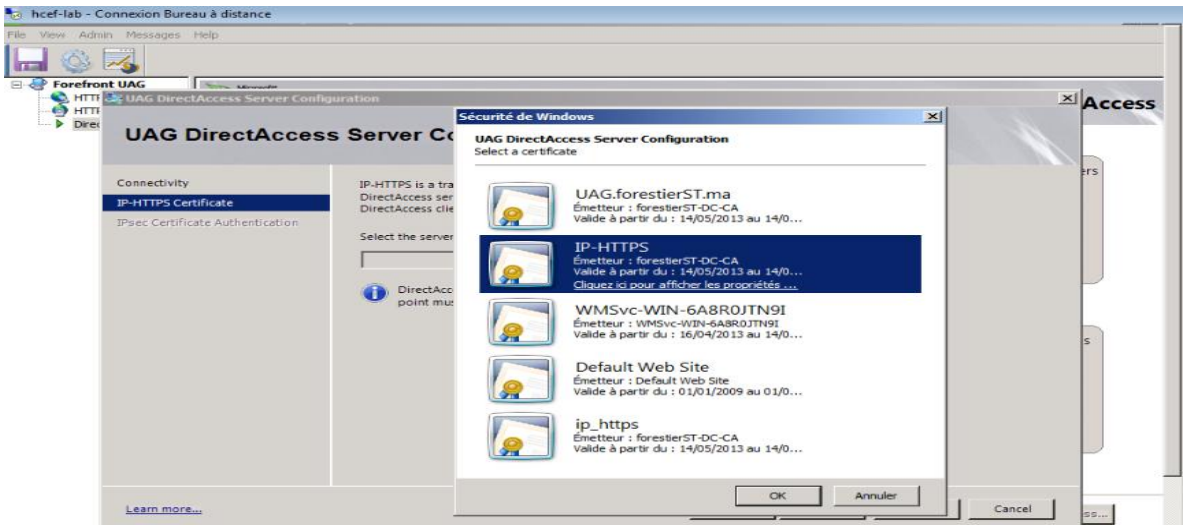

Figure n° 25: Certificat pour IP -HTTPs

Les clients DirectAccess nécessitent un certificat d'ordinateur pour établir un tunnel d'infrastructure IPsec, maintenant nous sommes appelées à sélectionner le CA qui va délivrer des certificats pour l'authentification IPsec.

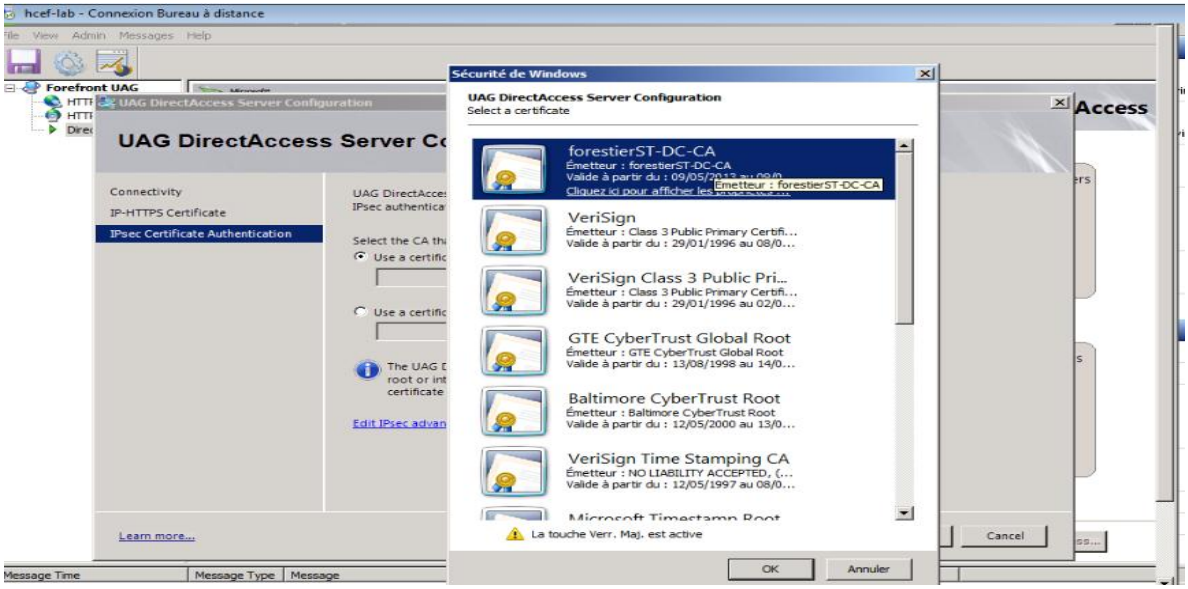

Figure n° 26: Certificat racine

Durant la prochaine étape, nous devons spécifier l'URL utilisé par les clients DirectAccess pour déterminer leur connectivité au réseau d'entreprise ou à Internet.

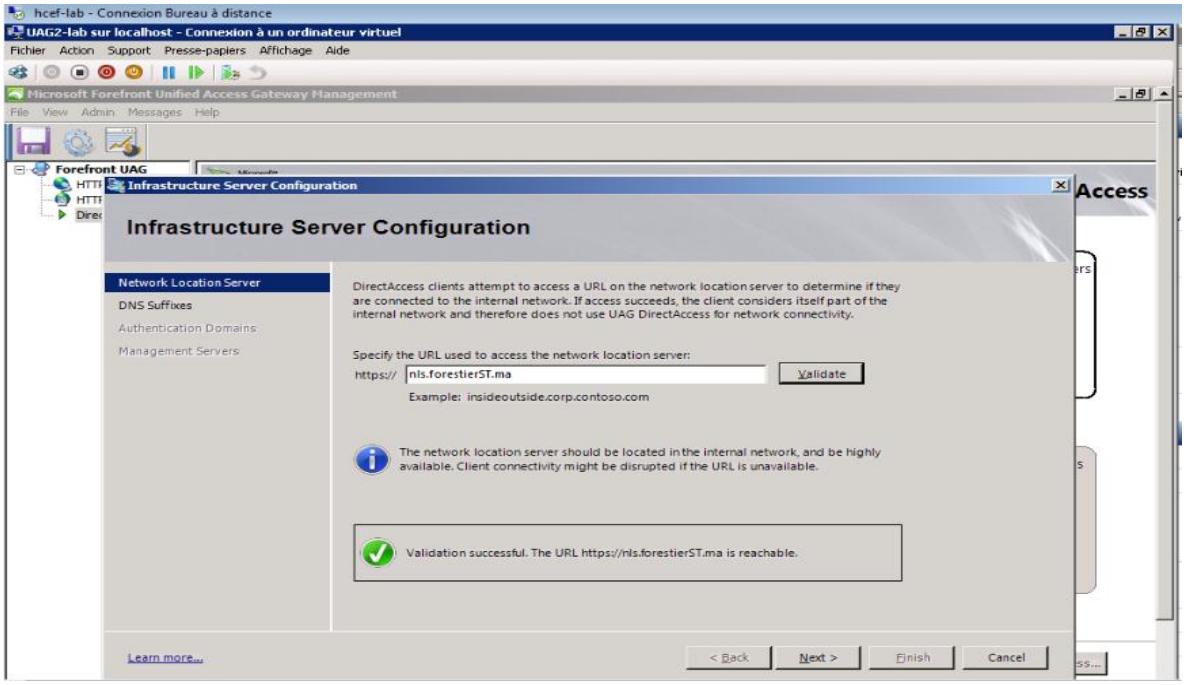

Figure n° 27: URL pour NLS

L’étape suivante est importante vu que durant elle que s’effectue la résolution des noms DNS internes pour les clients DirectAccess connectés à l'Internet. Les suffixes DNS que nous allons spécifier ici seront résolus par Forefront UAG DNS64.

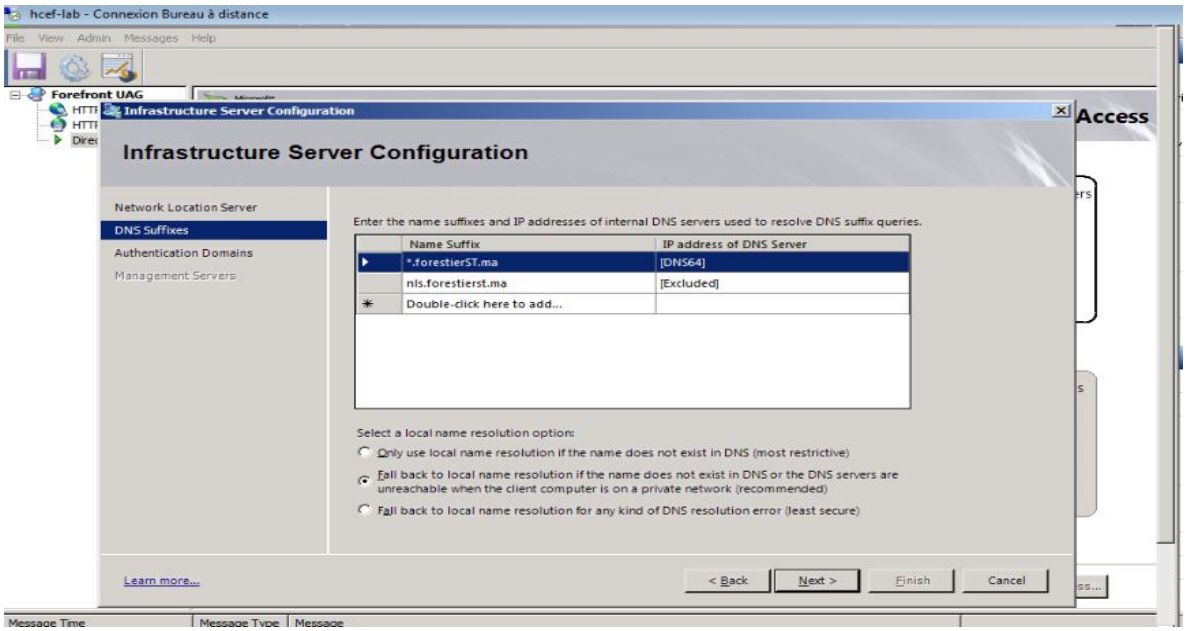

Figure n° 28: Résolution du nom via Forefront UAG

L’assistant suivant permet aux administrateurs d'ajouter des serveurs de gestion interne. Ces serveurs de gestion sont en mesure d'accéder au client DirectAccess après l’établissement du premier tunnel IPsec (le tunnel d'infrastructure) .

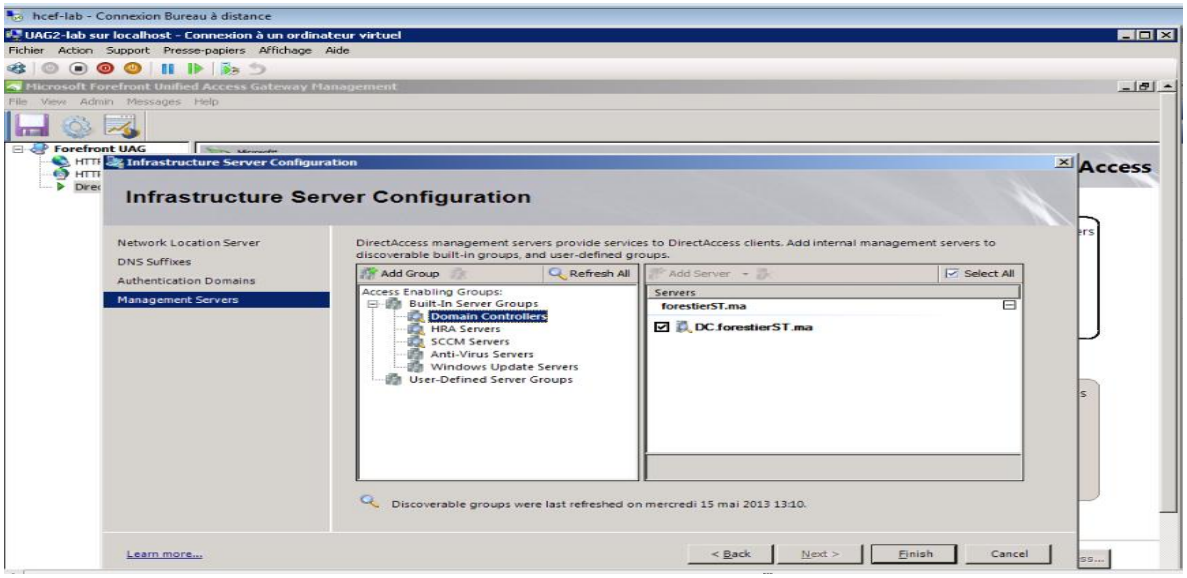

Figure n° 29: Liste des serveurs d'infrastructure

Après avoir fini les étapes de configuration avec succès, nous devons cliquer sur « Appliquer la stratégie ». Il est important de souligner à ce stade que Forefront UAG nous permet de revoir les étapes de configuration avant de créer les objets de stratégie du groupe.

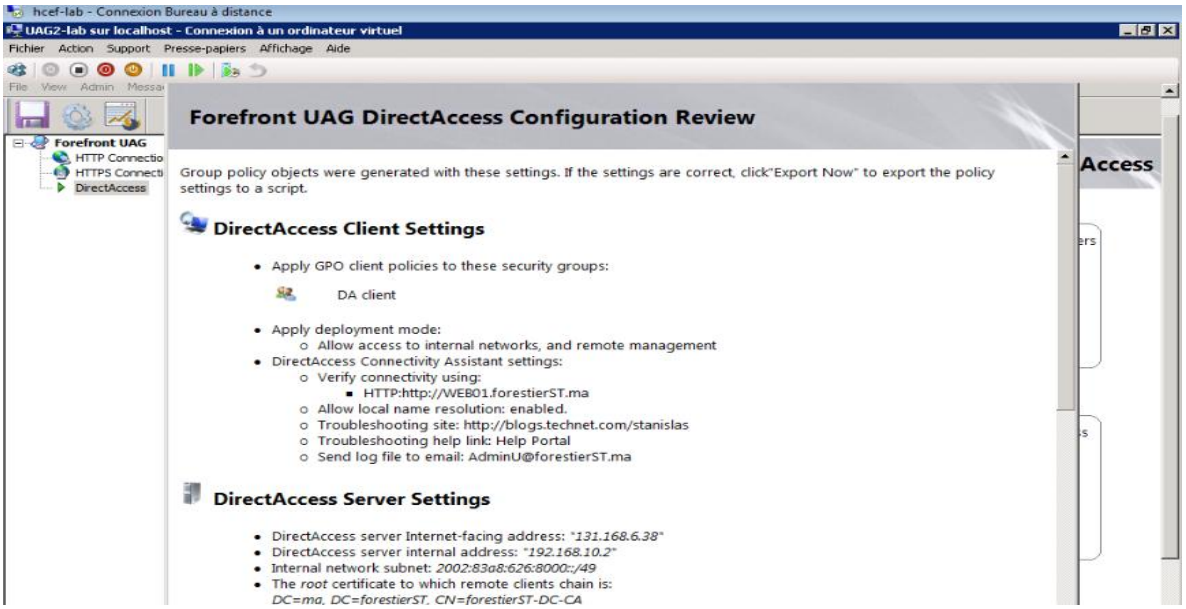

Figure n° 30: Paramètres de stratégie du groupe créé par DA

Pour effectuer un test, nous devons se connecter sur le poste client DirectAccess (connecté sur le LAN). Faire un Gpupdate / force pour appliquer la configuration DirectAccess. Déconnecter le client du LAN et le connecter sur le WAN (Internet). Ainsi, nous pouvons vérifier la connexion à une ressource interne fonctionne.

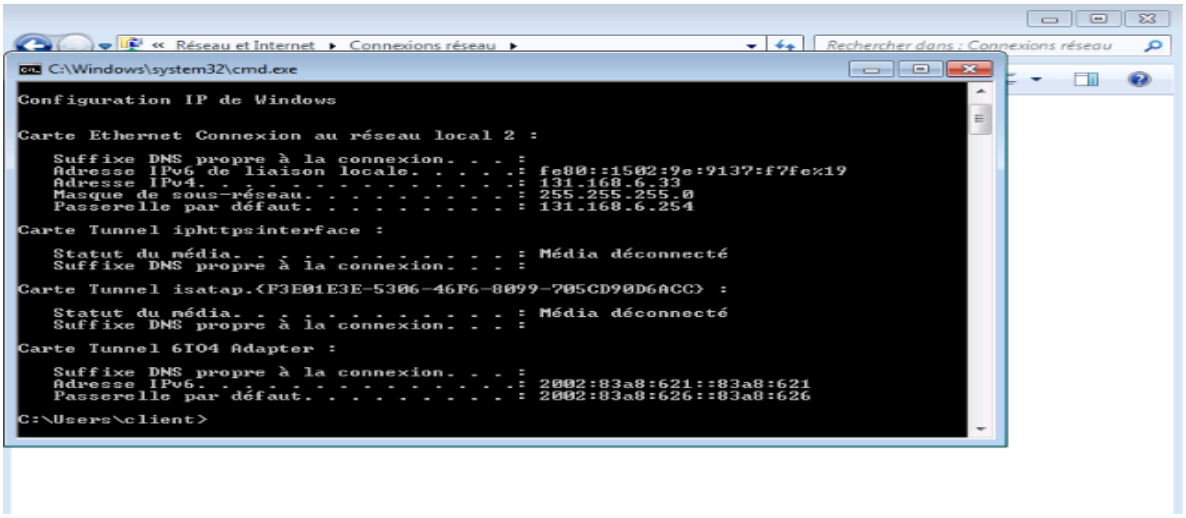

Figure n° 31: Test Client

Sur le serveur Forefront UAG, il est possible d'utiliser le Web Monitor pour vérifier le bon fonctionnement de DirectAccess :

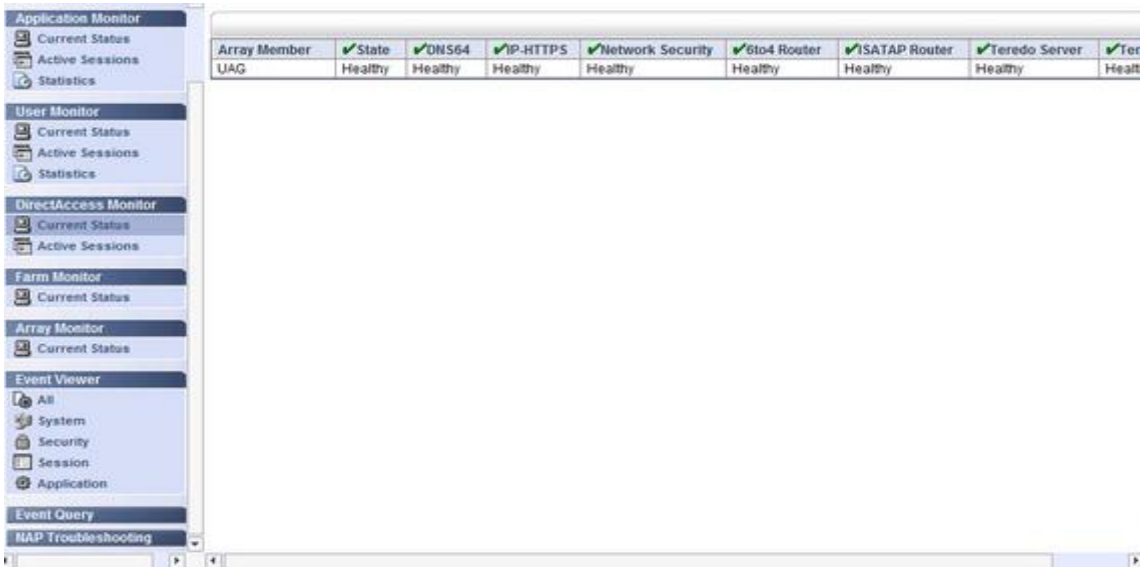

Figure n° 32: Web monitor

IV.2. Création d'un portail et publication

Dans cette phase nous allons créer un portail tronc HTTPS. Ce tronc portail sera utilisé pour publier des applications différentes.

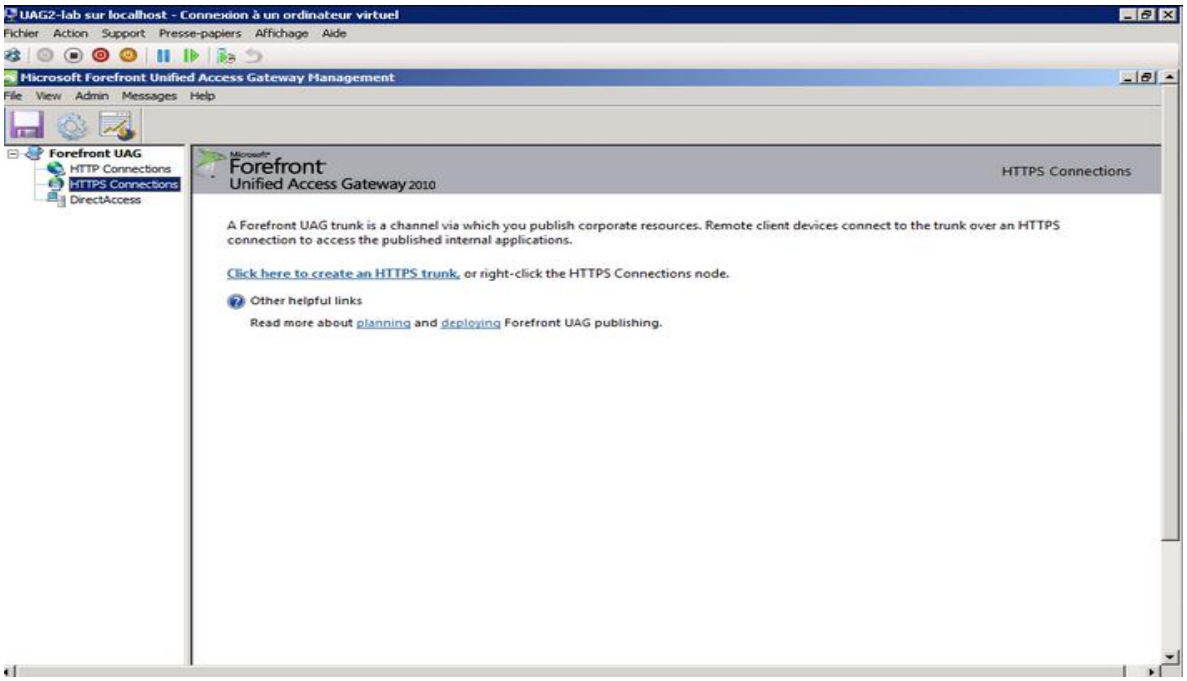

Figure n° 33: Portail vide

Avant de créer un nouveau portail, nous allons d'abord créer l'authentification et le référentiel d'autorisation. Dans notre cas, nous allons utiliser Active Directory en tant que fournisseur d'authentification.

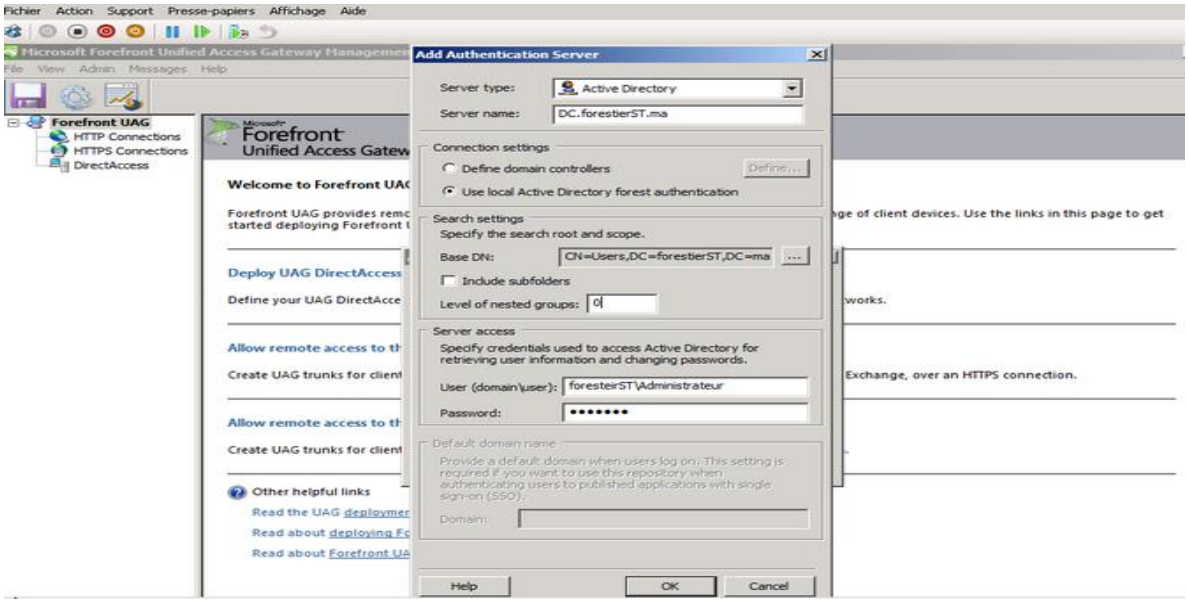

Figure n° 34: Configuration des serveurs d'autorisation

Après la configuration d'authentification avec succès, nous sommes en mesure de créer un nouveau portail.

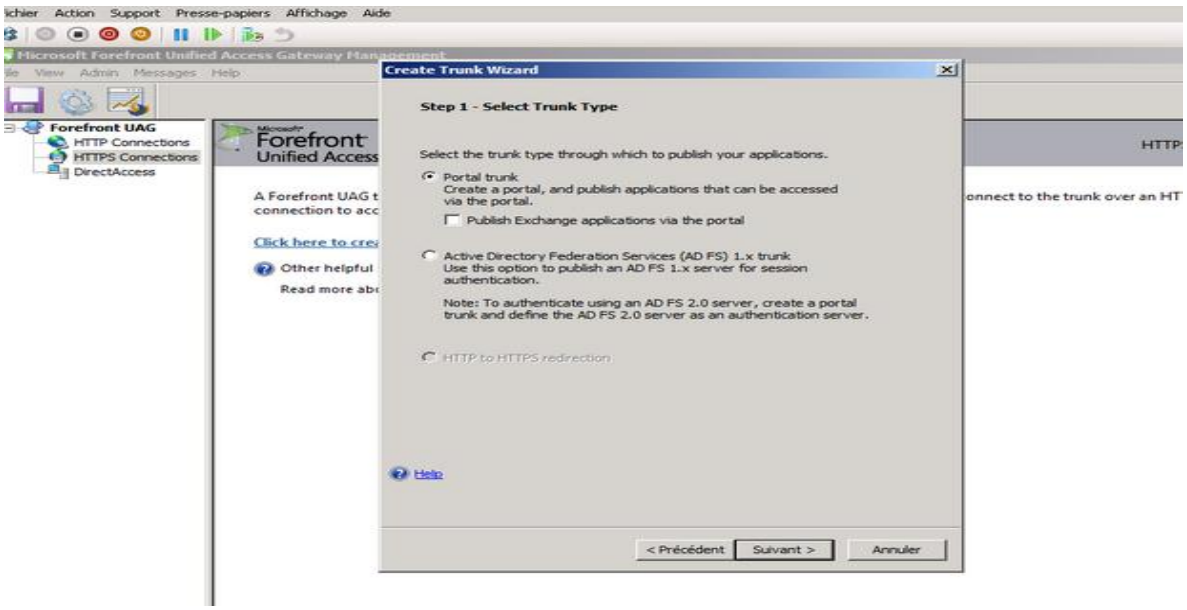

Figure n° 35: Création du Portail

Nous allons attribuer un nom au Portail et donner aussi un nom d'hôte public que les clients peuvent utiliser pour accéder au portail. Le nom d'hôte public doit correspondre au nom du certificat que nous utilisons pour la connexion HTTPS.

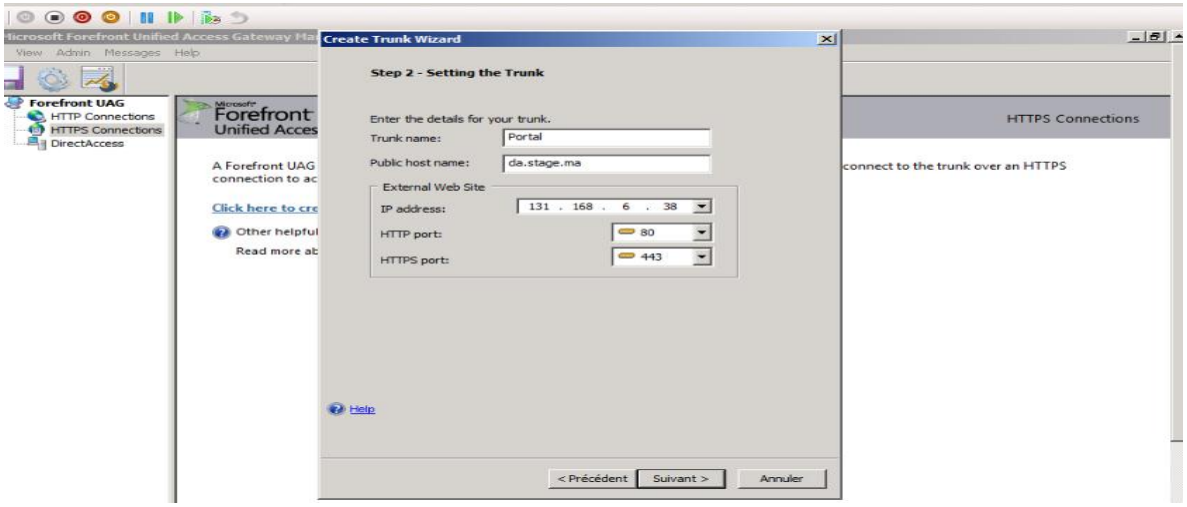

Figure n° 36: paramètre du portail

L'étape suivante consiste à sélectionner le certificat qui doit être utilisé pour établir la connexion SSL entre les clients externes et les Forefront UAG Server. Maintenant, il faut choisir la politique d'accès Endpoint UAG, nous pouvons utiliser NAP (protection d'accès au réseau) pour vérifier les clients avant qu'ils ne peuvent utiliser le portail.

Lorsque l'assistant est terminé, nous pouvons voir le portail crée comme il est indiqué sur la capture d'écran ci-dessous.

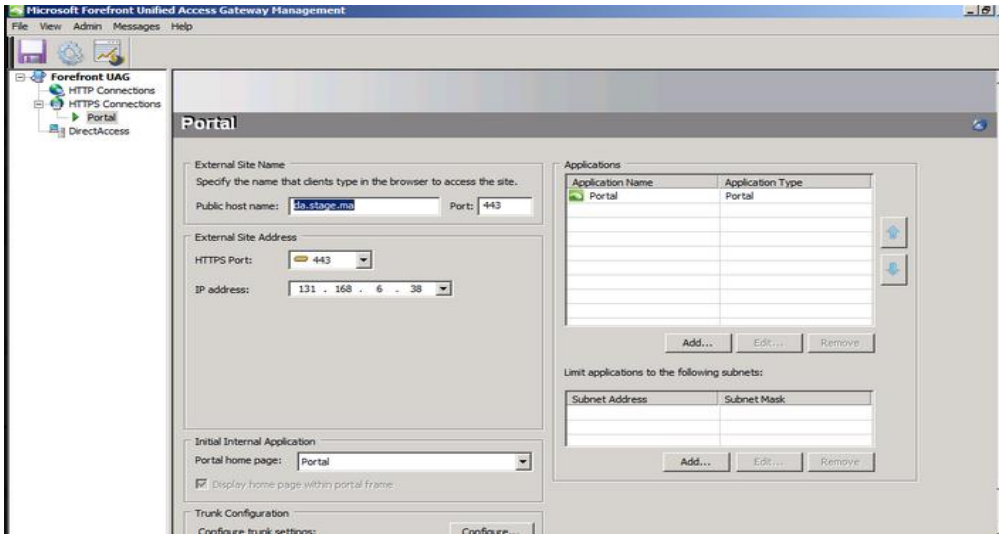

Figure n° 37: portail UAG

IV.2.1. Publication d'Exchange :

Pour publier un Microsoft Exchange Server 2010 Outlook Web App, Il faut se diriger vers le portail HTTPS créé à l'avance et cliquer sur « Ajouter » dans la fenêtre des applications.

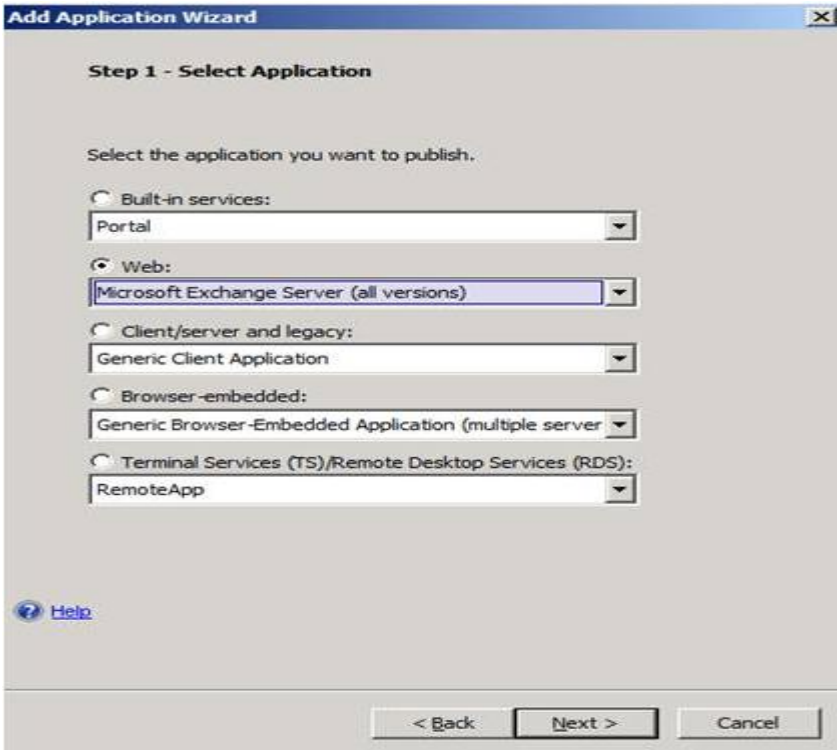

Figure n° 38: publication OWA via UAG

Il est nécessaire par la suite de donner un nom à la nouvelle application. Nous avons choisi de nommer l'application OWA, nous insérons également le nom de domaine complet interne de Microsoft Exchange Server 2010 et le port que nous souhaitons utiliser lorsque Forefront UAG doit accéder au serveur Exchange interne.

Dés que la configuration des paramètres s'achève, nous pouvons tester la connexion d'un client externe en ouvrant le site portail.

Figure n° 39: log On dans le portail UAG

Après l'authentification, nous pouvons accéder au portail UAG Forefront et utiliser donc l'application Web App Outlook publiée.

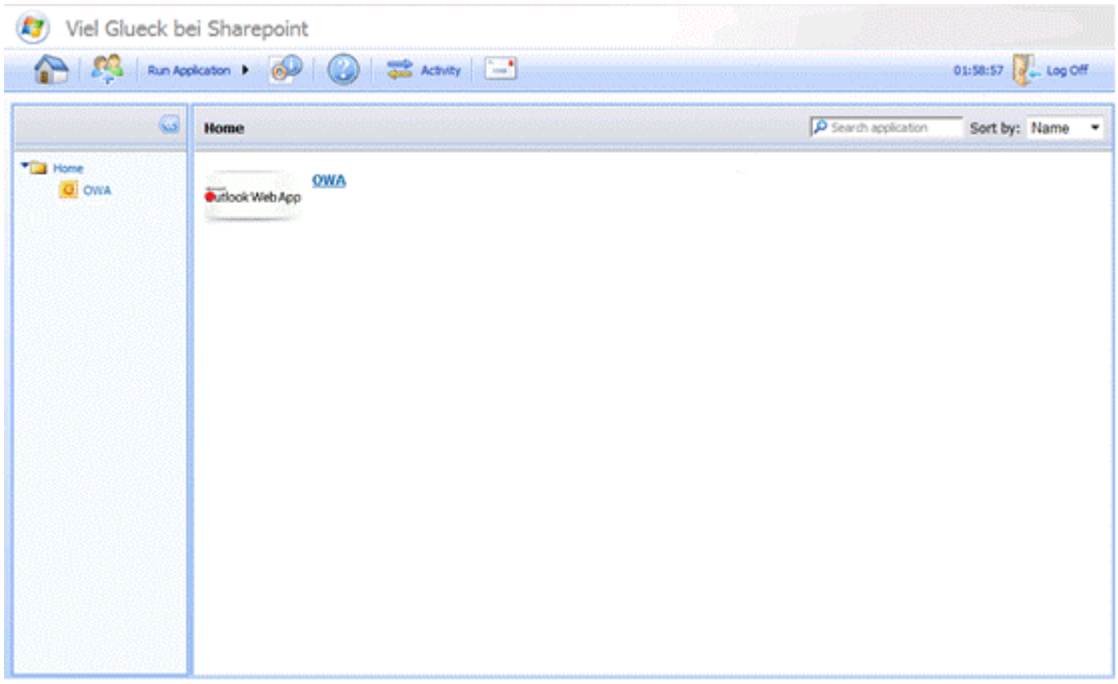

Figure n° 40: Access a OWA par portail

Partie II

Dans cette deuxième partie, nous allons présenter notre deuxième stage axé sur la modélisation du logiciel « Nagios » de supervision du Wi-Fi au sein de l'entreprise AZ-Net.

Chapitre I

Etude de l'existant

I. L'organisme d'accueil

AZ-Net est une société de service en Ingénierie Informatique (SSII), spécialisée dans l'installation et l'intégration des solutions de réseau et de sécurité informatique.

Depuis sa création en 2000, elle a toujours continué à offrir à ses clients des prestations d'installation « clé en main », conformément aux règles de l'art et selon la qualité requise, en incluant le câblage, l'installation et la configuration de matériels actifs pour le LAN, le WAN, l'accès à l'internet et la sécurité.

I.1. Fiche d'identité

- **Raison sociale:**

AZ-Net SARL

- **Création :**

Depuis Février 2000, AZ Net est au service de sa clientèle.

- **Certification :**

AZ Net est certifiée qualité ISO 9001 version 2000, par MOODY International, en Mars 2008.

- **Domaine de compétences :**

AZ Net est un intégrateur de solutions réseaux et télécoms multi-constructeurs et multiplateformes. Elle est spécialisée dans le domaine des réseaux informatiques et de la sécurité des systèmes d'information.

AZ-Net offre à sa clientèle une solution clé en main de la définition, de la solution, l'installation et la configuration, la mise en service et le déploiement, la formation, l'assistance et la maintenance ainsi que le service après-vente.

L'offre de cette société englobe également le Pré-câblage informatique, téléphonique et électrique, les réseaux sans fil (Wireless), les réseaux LAN et WAN, la sécurité informatique, la sauvegarde des données, la visioconférence et la vidéosurveillance.

- **Mission :**

Sa mission consiste à accompagner le client depuis la définition des besoins jusqu'à la réalisation de la solution convenant au mieux à l'infrastructure réseau informatique et télécom.

I.2. Activités

- Etude, installation et mise en œuvre des réseaux informatiques,
- Sécurité des systèmes informatiques,
- Aménagement des salles informatiques,
- Equipement des salles de conférence et visioconférence,
- Services d'accompagnement et de gestion.

II. Cahier des charges

II.1. Présentation du projet

Les performances d'un réseau sans fils dépendent de plusieurs critères. Nous pouvons citer les plus importants de ces critères tels que le temps nécessaire pour le traverser, le débit nominal, le taux de perte des données.

Afin de mesurer les performances, il est nécessaire de superviser les principales valeurs qui permettent de qualifier le réseau sans fils.

La supervision est une technologie qui permet de suivre le fonctionnement et l'évolution d'un processus dans le temps.

Dans notre cas, nous utilisons la supervision afin d'observer et d'analyser le fonctionnement des réseaux sans fils.

La supervision comporte plusieurs processus de fonctionnement :

- La collection de l'information,
- L'archivage de l'information collectée,
- La restitution et la transformation de l'information afin d'être interprété.

II.1.1. L'intérêt du projet

Afin d'apporter une amélioration à un logiciel de supervision open-source « Nagios », et de pouvoir ainsi superviser les réseaux sans fil « Wi-Fi » contrôlé via un contrôleur ZoneDirector « ruckus », il faut mettre en place un logiciel de supervision « Nagios » et développer des plugins pour pouvoir superviser le réseau Wi-Fi.

II.2. La problématique du projet

Les technologies radio supportent des flux de données liées à des fonctions de plus en plus stratégiques et complexes au sein des entreprises. Aujourd'hui, de nombreuses sociétés utilisent les réseaux Wi-Fi sans disposer d'alternative filaire.

Il est donc primordial pour les administrateurs réseaux d'avoir une vue globale et instantanée sur l'ensemble du réseau, d'où le besoin d'avoir un logiciel de supervision des réseaux Wi-Fi. Mais dans le cas des produits open-source, cette solution reste encore couteuse et indisponible.

II.3. L'objectif du projet

L'analyse de l'expression des besoins a abouti à la détermination de l'objectif de notre action que nous pouvons résumer dans le fait de modifier le code en langage de programmation « Perl » du plugin « Zone Director » chose qui permet de lier le contrôleur Wi-Fi « Ruckus » au logiciel « Nagios » et ce en vue de superviser les différentes fonctionnalités du réseau. Par ailleurs, créer des Templates en « PHP » et en générer des fichiers « XML » est une opération qui permet d'afficher les graphes associés à la fonctionnalité ajoutée.

III. Planification du projet

III.1. Cycle de vie du projet

III.1.1. Spécification des besoins du projet

Cette étape consiste à identifier les besoins, les analyser et les classer/prioriser.

L'identification des besoins est une méthode de réflexion qui donne la chance d'analyser et de quantifier les besoins à satisfaire, avec si possible leur hiérarchisation par ordre de priorité (priorisation des besoins). Elle exige la collecte des données disponibles ainsi qu'un travail de concertation et de consultation avec la direction Technico-commerciale. Cette phase se chevauche en général avec la phase suivante (analyse des données).

III.1.2. Analyse

Cette étape consiste à étudier tous les aspects de la modélisation du logiciel « Nagios » pour s'assurer de sa viabilité et à planifier aussi, tout le processus de sa mise en œuvre afin que le projet soit réalisé dans les délais voulus et qu'il atteigne les résultats attendus.

III.1.3. Installation et Configuration

Cette étape consiste à mettre en place le logiciel « Nagios » et le configurer afin de pouvoir superviser le réseau d'une manière globale et dans un temps réduit.

III.1.4. Développement

Appelée aussi codage, implémentation ou programmation, cette phase assure la traduction dans un langage de programmation des fonctionnalités.

III.1.5. Test

Les tests permettent de vérifier individuellement que chaque fonctionnalité ajoutée au logiciel « Nagios » est implémentée conformément aux spécifications des besoins.

Généralement, après la vérification effectuée à l'aide des tests. L'équipe de l'entreprise veillent à contrôler les différents éléments (modules) ajoutés au logiciel « Nagios ». Pour suivre l'exécution du projet et s'assurer du degré d'aboutie des objectifs et d'apporter aussi les corrections nécessaires en temps voulu.

III.1.6. Livraison

Durant cette étape nous livrons le produit au client (dans notre cas il s'agit de l'entreprise AZ-Net) pour qu'il puisse l'utiliser et l'exploiter à sa guise.

III.1.7. Maintenance

Cette phase comprend toutes les actions correctives « maintenance corrective » et évolutives « maintenance évolutive » sur l'application.

Pour élaborer notre projet, nous avons adopté le cycle de vie suivant :

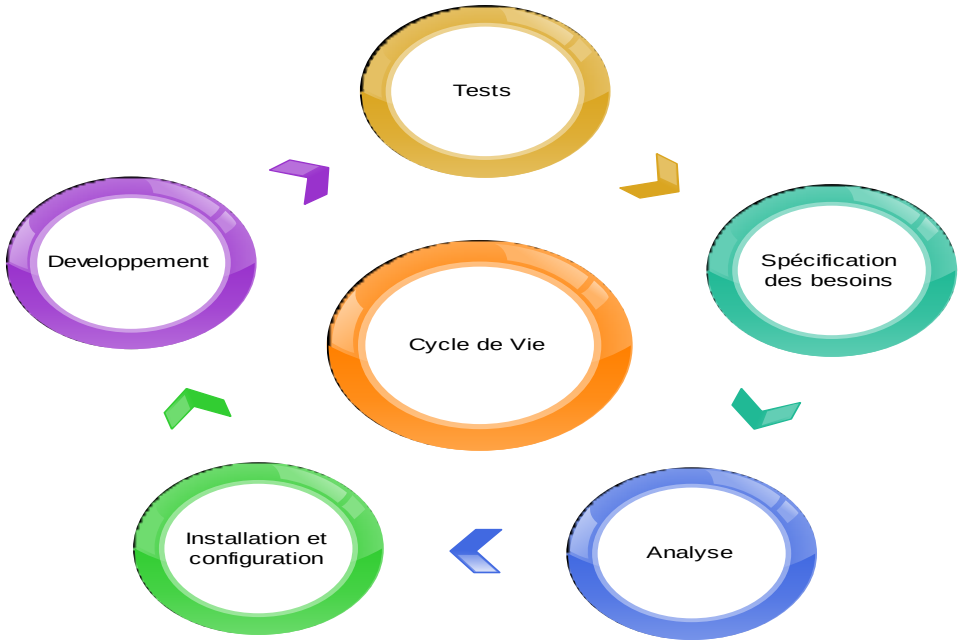

Figure I. 1: Cycle de Vie

III.2. Product BreakDown Structure(PBS)

Product BreakDown Structure (PBS) : est la « structure de décomposition par produit » constituant le squelette du projet, elle considère le résultat final du projet comme un « produit », c'est à dire tel une réalisation que nous donnons en main propre au client après la fin du projet. Nous déduisons donc, que le produit constitue l'objectif du projet.

Le squelette ci-dessous représente la structure de décomposition par produit de notre projet.

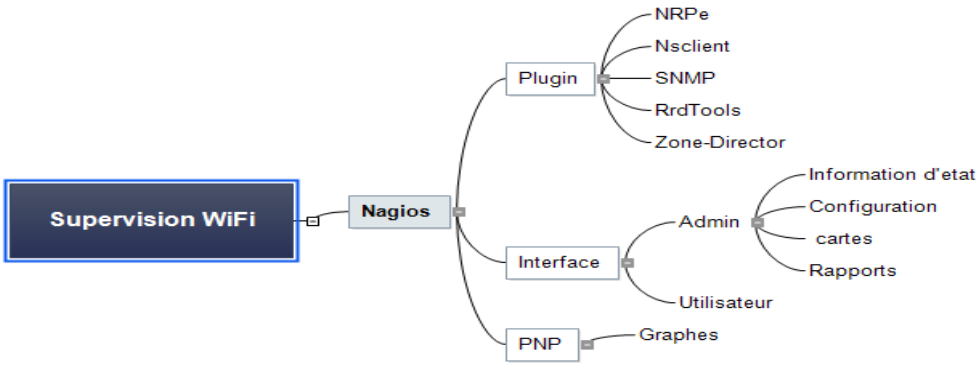

Figure I. 2: Product BreakDown Structure

III.3. Work Breakdown Structure (WBS)

WorkBreakdown Structure (WBS) : est la « structure de décomposition par tâches » Elle constitue la « musculature » du projet. Son rôle consiste à contrôler l'ensemble des tâches qui doivent être réalisées. Pour s'assurer du fait que chaque objectif final et même sous objectif soient atteints vers la fin du projet du projet.

Le schéma ci-dessous présente la structure de décomposition par tâches de notre projet.

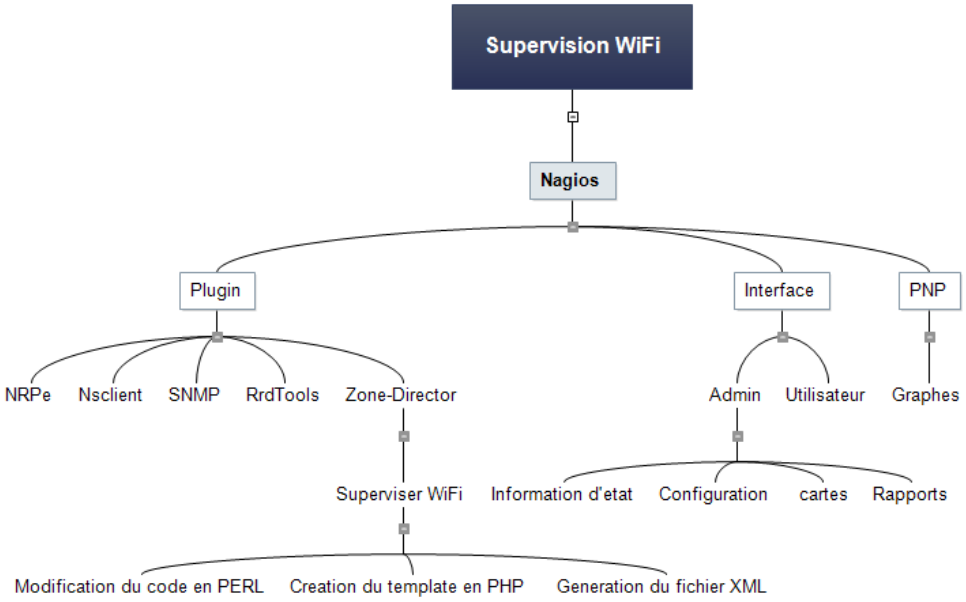

Figure I. 3: Work BreakDown Structure

III.4. Diagramme de GANTT

Nous disposons de trois mois pour effectuer notre stage, nous avons opté alors, pour une planification minutieuse dès le début du projet, ce qui nous a permis de dresser un inventaire des tâches à accomplir. Dans ce sens, nous avons estimé la durée et la dépendance des tâches en fonction de l'expérience acquise lors de nos précédents stages et projets.

Le diagramme de Gantt ci-dessous illustre les différentes itérations de notre projet avec leur taux de finalisation.

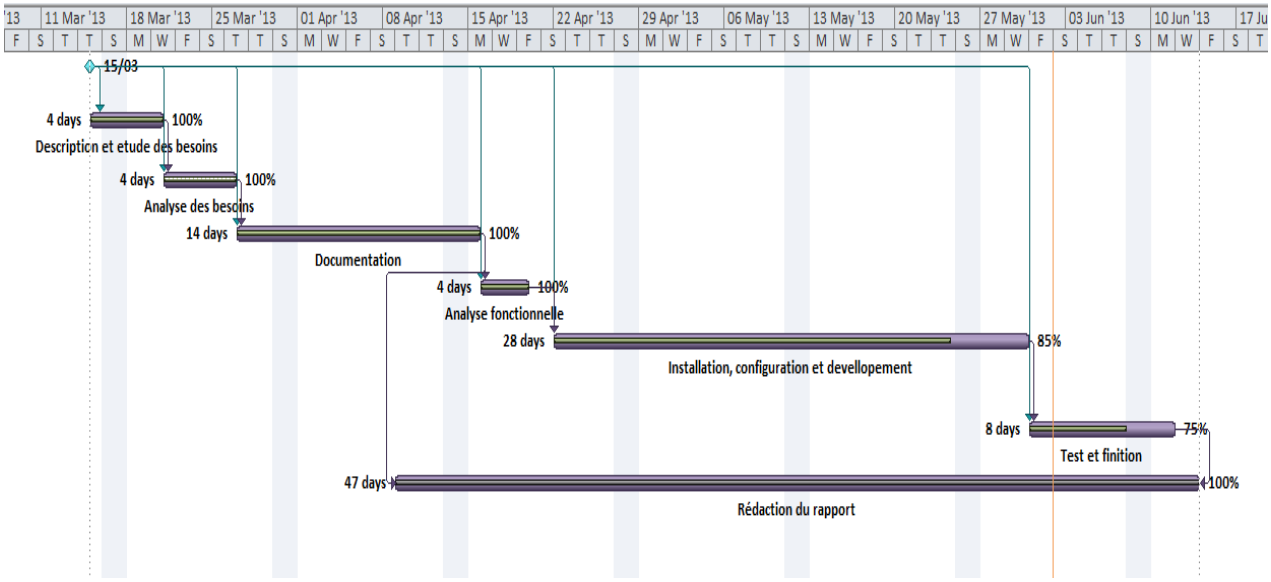

Figure I. 4: Diagramme de GANTT

Chapitre II

Généralités

I. Le réseau local sans fil : Wi-Fi

Le Wi-Fi est une technologie de réseau informatique sans fil mise en place pour fonctionner en réseau interne et, depuis, devenue un moyen d'accès à haut débit à internet. Il est basé sur la norme IEEE 802.11.

Dans la pratique, le wifi permet de relier des ordinateurs portables, des machines de bureau, des assistants personnels (PDA), des objets communicants ou même des périphériques à une liaison haut débit (de 11 Mbit/s en 802.11b à 54 Mbit/s en 802.11a/g) sur un rayon de plusieurs dizaines de mètres en intérieur (généralement entre une vingtaine et une cinquantaine de mètres). Dans un environnement ouvert, la portée peut atteindre plusieurs centaines de mètres voire plusieurs dizaines de kilomètres (pour la 'variante' WIMAX ou avec des antennes directionnelles) dans des conditions optimales.

I.1. Mode opératoires du réseau 802.11

Le Wi-Fi cible deux contextes d'utilisation distincts pour un réseau Wi-Fi ayant chacun des caractéristiques propres. Il s'agit du mode **infrastructure** et du mode **ad hoc** (sans infrastructure). Ces deux modes de fonctionnement permettent de définir la topologie du réseau sans fil. La figure ci-dessous représente brièvement les modes de fonctionnement d'un réseau Wi-Fi.

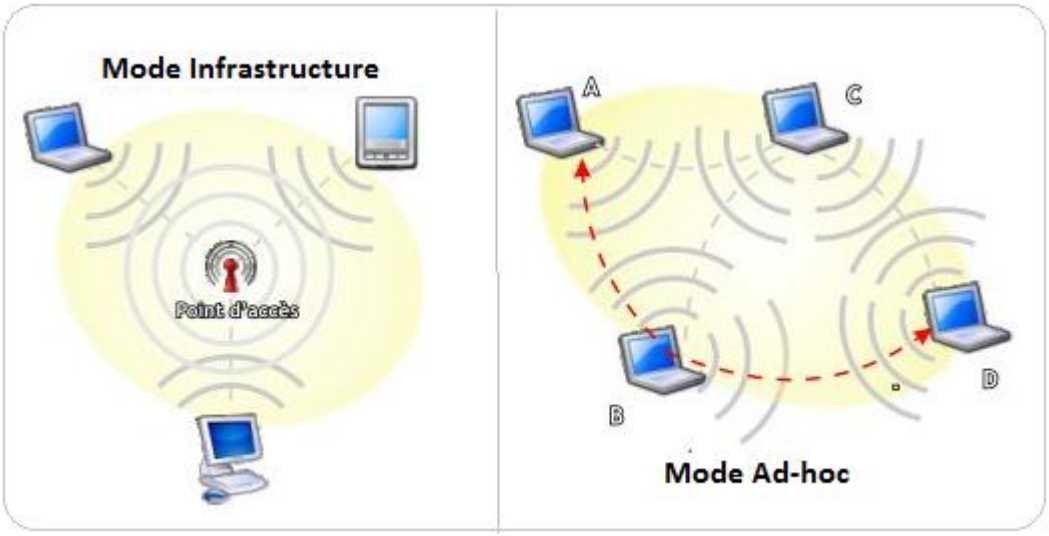

Figure II. 1: Mode opératoire du réseau Wi-Fi

I.2. Architecture du Wi-Fi

La norme 802.11 s'attache à définir les couches basses du modèle OSI pour une liaison sans fil utilisant des ondes électromagnétiques, autrement dit :

- **La couche physique** (notée parfois couche PHY), propose trois types de codage de l'information,

- **La couche liaison de données**, constituée de deux sous-couches : le contrôle de la liaison logique (Logical Link Control, ou LLC) et le contrôle d'accès au support (Media Access Control, ou MAC).

La couche physique définit la modulation des ondes radio-électriques et les caractéristiques de la signalisation pour la transmission des données. Tandis que la couche liaison de données définit l'interface entre le bus de la machine et la couche physique. Elle possède notamment une méthode d'accès proche de celle utilisée dans le standard Ethernet et elle s'appuie dans sa fonction sur les règles de communication entre les différentes stations.

I.3. Les différentes normes Wi-Fi

La norme IEEE 802.11 est en réalité la norme initiale offrant des débits de 1 ou 2 Mbps. Des révisions ont été apportées à la norme originale afin d'optimiser le débit (c'est le cas

des normes 802.11a, 802.11b et 802.11g, appelées normes 802.11 physiques) et aussi pour préciser des éléments dans le but d'assurer une meilleure sécurité ou une meilleure interopérabilité. Vous trouvez dans la page suivante un tableau présentant les différentes révisions de la norme 802.11 et leur signification :

Norme	***Nom***	***Description***
802.11a	**Wi-Fi5**	La norme 802.11 a permet d'obtenir un haut débit (54 Mbps théoriques, 30 Mbps réels). La norme 802.11a spécifie 8 canaux radio dans la bande de fréquence des 5 GHz.
802.11b	**Wi-Fi**	La norme 802.11b est la norme la plus répandue actuellement. Elle propose un débit théorique de 11 Mbps (6 Mbps réels) avec une portée pouvant aller jusqu'à 300 mètres dans un environnement dégagé. La plage de fréquence utilisée est la bande des 2.4 GHz, avec 3 canaux radios disponibles.
802.11c	**Pontage 802.11 vers 802.1d**	Il s'agit uniquement d'une modification de la norme 802.1d afin de pouvoir établir un pont avec les trames 802.11 (niveau liaison de données).
802.11d	**Internationalisation**	La norme 802.11d est un supplément à la norme 802.11 dont le but est de permettre une utilisation internationale des réseaux locaux 802.11.
802.11e	**Amélioration de la qualité de service**	La norme 802.11e vise à donner des possibilités en matière de qualité du service au niveau de la couche liaison de données. Ainsi cette norme a pour but de définir les besoins des différents paquets en termes de bande passante et de délai de transmission de manière à permettre une meilleure transmission de la voix et de la vidéo.
802.11f	**Itinérance (roaming)**	La norme 802.11f est une recommandation à l'intention des vendeurs de point d'accès pour une meilleure interopérabilité des produits. Elle propose le protocole Inter-Access point roaming protocol permettant à un utilisateur itinérant de changer de point d'accès de façon transparente lors d'un déplacement, quelles que soient les marques des points d'accès présentes dans l'infrastructure réseau.
802.11g		La norme 802.11g est la plus répandue dans le commerce actuellement. Elle a une compatibilité descendante avec la norme802.11b.Et elle offre un haut débit: 54 Mbit/s théoriques, 26 Mbit/s réels sur la bande de fréquences des 2,4 GHz.

802.11h		La norme 802.11h vise à rapprocher la norme 802.11 du standard Européen (HiperLAN 2, d'où le h de 802.11h) et cherche à être en conformité avec la réglementation européenne en matière de fréquence. et d'économie d'énergie.
802.11i		La norme 802.11i a pour but d'améliorer la sécurité des transmissions (gestion et distribution des clés, chiffrement et authentification). Cette norme s'appuie sur l'AES (Advanced Encryption Standard) et propose un chiffrement des communications pour les transmissions utilisant les technologies 802.11a, 802.11b et 802.11g.
802.11n	**WWiSE (World-Wide Spectrum Efficiency) ou TGn Sync**	La norme 802n est sortie en 2007 son débit théorique atteint les 540 Mbit/s (débit réel de 100Mbit/s) avec une portée de rayon de 90 mètres grâce aux technologies MIMO (multiple-input multiple-output) et OFDM (Orthogonal Frequency Division Multiplexing).
802.11s	**Réseau Mesh**	La norme 802.11s est en cours d'élaboration. Son débit théorique atteint aujourd'hui 1 à 2 Mbit/s, et son but est d'implémenter la mobilité sur les réseaux de type ad hoc.

Tableau II. 1: Les différentes normes Wi-Fi

I.4. Les équipements Wi-Fi

Il existe différents types d'équipement pour la mise en place d'un réseau sans fil Wifi :

- **Les adaptateurs sans fil ou cartes d'accès :** Il s'agit d'une carte réseau à la norme 802.11 permettant à une machine de se connecter à un réseau sans fil. Les adaptateurs Wi-Fi sont disponibles dans de nombreux formats (carte PCI, carte PCMCIA, adaptateur USB, carte compact flash, ...). D'ailleurs nous appelons station tout équipement possédant une telle carte. Il est important de souligner que les composants Wi-Fi deviennent des standards sur les portables.).
- **Les points d'accès :** Notés AP pour Access point, parfois appelés bornes sans fil. Ils permettent de fournir au réseau filaire un accès (auquel ils sont raccordés) aux différentes stations avoisinantes équipées de cartes Wi-Fi. Cette sorte de hub est l'élément nécessaire pour déployer un réseau centralisé en mode infrastructure. Certains modèles proposent des fonctions de modem ADSL et d'autres, fonctions comme un pare-feu.

- **Les autres :**

  - **Smart Display** : écrans mobiles, soutenus par Microsoft.

  - **Chaînes Wi-Fi** : offrant la capacité de lire les MP3 directement sur le disque dur d'un ordinateur grâce à l'interface Ethernet sans fil intégrée. Elle préfigure toute une génération de produits, capables de lire, outre les CD audio, les radios qui émettent en MP3 sur internet.

  - **Assistant personnel:** les PDA intégrant le Wi-Fi sont parfois plus avantageux qu'un portable pour lire les mails, importer des documents voir surfer sur le net.

  - **Rétroprojecteurs:** pour des présentations avec portables mobiles.

  - **Caméra vidéo:** transmet des images à distance à l'ordinateur qui les enregistre par la suite.

II. Sécurité des réseaux Wi-Fi :

Les ondes radio-électriques ont intrinsèquement une grande capacité à se propager dans toutes les directions avec une portée relativement grande. Il est ainsi, très difficile d'arriver à confiner les émissions d'ondes radio dans un périmètre restreint.

La principale conséquence de cette "propagation sauvage" des ondes radios est la facilité d'accès que peut avoir une personne non autorisée d'écouter le réseau. Il existe plusieurs niveaux de sécurité permettant d'une part, de gérer les droits d'accès au réseau Wi-Fi, et d'autre part, de garantir la confidentialité des échanges.

II.1. Infrastructure adaptée :

Dans cette perspective, la première action à effectuer consiste à positionner intelligemment les points d'accès selon la zone à couvrir. Il est préférable d'éviter les murs extérieurs et de choisir plutôt un emplacement central.

II.2. Eviter les valeurs par défauts :

Lors de la première installation d'un point d'accès, celui-ci est configuré avec des valeurs par défaut, y compris en ce qui concerne le mot de passe de l'administrateur. Toutefois, les paramètres par défaut agissent de façon que la sécurité soit minimale. Il est donc impératif de se connecter à l'interface d'administration pour définir un mot de passe

d'administration.

En outre, afin de se connecter à un point d'accès il est indispensable de connaître l'identifiant du réseau (SSID). Ainsi qu'il est vivement conseillé de modifier le nom de réseau par défaut et de désactiver la diffusion.

II.3. Chiffrement WEP ou WPA

Pour remédier aux problèmes de confidentialité des échanges sur les réseaux sans fils, le standard 802.11 intègre un mécanisme simple de chiffrement des données, il s'agit du WEP, qui est un protocole chargé du chiffrement des trames 802.11 utilisant l'algorithme symétrique RC4 avec des clés d'une longueur de 64 bits ou 128 bits.

Par ailleurs, pour obtenir un niveau de sécurité supérieur, il convient d'utiliser le cryptage WPA ou WPA2.

II.4. Filtrage des adresses MAC

Chaque adaptateur réseau possède une adresse physique qui lui est propre (appelée adresse MAC). Cette adresse est représentée par 12 chiffres hexadécimaux groupés par paires et séparés par des tirets. Les points d'accès permettent généralement dans leur interface de configuration de gérer une liste de droits d'accès (appelée ACL) basée sur les adresses MAC des équipements autorisés à se connecter au réseau sans fil. En activant ce MAC Adresse Filtering (Filtrage des adresses MAC), même si cette précaution est un peu contraignante, nous pouvons limiter l'accès au réseau à un certain nombre de machines. En contrepartie, cette démarche ne règle pas le problème de la confidentialité des échanges.

II.5. Amélioration de l'authentification

Afin de gérer plus efficacement les authentifications, les autorisations et la gestion des comptes utilisateurs (en anglais AAA pour Authentication, Authorization, and Accounting) il est possible de recourir à un serveur RADIUS (Remote Authentication Dial-In User Service). Le protocole, est un système client/serveur permettant de gérer de façon centralisée les comptes des utilisateurs et les droits d'accès associés.

III. Supervision du Wi-Fi

La supervision de réseaux peut être définie comme l'utilisation de ressources réseaux adaptées dans le but d'obtenir des informations (en temps réel ou non) par interrogation périodique ou par remontée non sollicitée de l'informations de la part des équipements de réseau, sur l'utilisation ou la condition des réseaux et de leurs éléments afin d'assurer un niveau de service garanti, une bonne qualité et une répartition optimale.

La mise en place d'une supervision réseau a comme principale vocation la collection, à intervalle régulier, des informations nécessaires sur l'état de l'infrastructure et des entités qui y sont utilisées, de les analyser et de les rapporter.

Il existe des protocoles réseau qui permettent de récupérer des informations sur le parc informatique. Les deux plus importants qui possèdent des rôles très différents mais qui ont un point en commun : Ils sont tous deux largement utilisés par les logiciels de supervision.

- **ICMP (Internet Control Message Protocol) :** est un protocole de couche réseau qui vient palier à l'absence de message d'erreur du protocole IP (Internet Protocol). C'est un protocole très simple, qui n'a pas pour fonction directe la supervision d'un réseau mais qui est utilisé comme source d'information sur la qualité du réseau ou sur la présence d'une machine.

- **SNMP (Simple Network Management Protocol) :** SNMP signifie Simple Network Management Protocol (protocole simple de gestion de réseau). C'est un protocole qui permet comme son nom l'indique, de gérer les équipements réseaux ainsi que les machines informatiques. Ce protocole est donc utilisé par les administrateurs réseaux pour détecter à distance les problèmes qui surviennent sur leur réseau. Par soucis de simplicité et donc de rapidité, SNMP ne transporte que des variables et s'appuie sur le protocole UDP (User Datagram Protocol). SNMP va créer un dialogue entre des agents installés sur des machines à superviser et un serveur de supervision. Les échanges entre agents et serveur se résument à trois opérations, les alarmes, les requêtes et les réponses :

    - Une requête est émise du serveur vers un agent via le port 161 UDP si le serveur veut demander ou imposer quelque chose à cet agent. La requête peut être de quatre types :

- **GetRequest** : Demande la valeur d'une variable à un agent ;
- **GetNextRequest** : Demande la valeur suivante de la variable ;
- **GetBulk** : Demande un ensemble de variables regroupées ;
- **SetRequest** : Demande la modification de la valeur d'une variable .

- L'agent va ensuite traiter cette requête et émettre une réponse via le même port. Si tout se passe bien, l'agent répond un GetResponse accompagné de la valeur demandée. Mais dans le cas contraire l'agent ajoutera un code d'erreur en réponse (par exemple No Access ou Read Only).

- Une alarme est créée par un agent en cas d'évènement et utilise un message dit de type trap ou de type inform pour prévenir le serveur. Ce message SNMP transite via le port 162 UDP.

Dans notre cas, nous allons configurer le logiciel « Nagios » qui se base sur le protocole SNMP, pour pouvoir superviser le réseau Wi-Fi.

III.1. C'est quoi Nagios ?

Nagios est un logiciel libre distribué sous licence GPL. Il permet de superviser un système d'information complet utilisé par de nombreuses sociétés.

Etant le successeur de **NetSaint** ,Nagios est considéré comme une évolution de ce dernier avec l'ajout en principe de la gestion du protocole SNMP.

Cet outil repose sur une plate-forme de supervision, fonctionnant sous Linux et sous la plupart des systèmes Unix. Grace à son fonctionnement modulaire, il centralise les informations récoltées périodiquement. Chose qui le rend beaucoup plus attractif que les autres produits concurrents bien que, sa configuration se révéle complexe.

III.1.1. Fonctionnalités

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

- La supervision des services réseaux (SMTP, HTTP,…), des hôtes et des ressources systèmes (CPU, charge mémoire…),

- La détermination à distance et de manière automatique de l'état des objets et des ressources nécessaires au bon fonctionnement du système grâce à ses plugins. Les plugins sont écrits dans les langages de programmation les plus adaptés à leur tâche (Bash, C++, Python, Perl, PHP, C#, etc.),
- Représentation coloriée des états des services et des hôtes définies,
- Génération de rapports,
- Cartographie du réseau,
- Gestion des alertes,
- Surveillance des processus (sous Windows, Unix…),
- La supervision à distance peut utiliser SSH ou un tunnel SSL.

Figure II. 2: Centralisation de l'information par Nagios

III.1.2. Architecture

L'architecture de Nagios se base sur le paradigme serveur-agent. Cet outil s'appuie spécifiquement sur un 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 en trois parties coopératives que nous décrivons dans les points suivants :

- **Un noyau** : qui est le cœur du serveur Nagios, lancé sous forme de démon. Il est responsable de la collecte et de l'analyse des informations, de la réaction, de la prévention, de la réparation et de l'ordonnancement des vérifications (quand et dans quel ordre) ;

- **Des exécutants** : ce sont les plugins, responsables de l'exécution des contrôles et des tests sur des machines distantes ou locales et du renvoi des résultats au noyau du serveur Nagios ;

- **L'interface graphique :** accessible par le web, elle est conçue pour rendre plus exploitable les résultats. Cette interface est basée sur les CGI (Common Gateway Interface) fournis par défaut lors de l'installation de Nagios et qui interprètent les réponses des plugins pour les présenter dans l'interface par la suite.

Figure II. 3 : Architecture de Nagios

III.1.3. Plugins

Nagios fonctionne grâce à des plugins écris en Perl ou en C. Sans ces plugins Nagios incapable de superviser et il se réduit à un simple noyau.

Les plugins sont en fait, 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 des requêtes vers les hôtes ou les services choisis lors d'un appel du processus de Nagios. Et il se base sur la transmission du code de retour au serveur principal qui par son tour se charge d'interpréter les résultats et de déterminer l'état de l'entité réseau testée.

Il est possible de créer son propre plugin et de l'interfacer avec Nagios tout en respectant les conventions des codes de retour que nous allons expliquer par la suite.

La relation entre le noyau et les plugins est assurée d'une part par les fichiers de configuration (définitions des commandes) et d'autre part, par le code retour d'un plugin.

Le tableau suivant présente un résumé de cette relation:

Code retour	*Etat*	*Signification*
1	OK	Tout va bien
2	Warning	Le seuil d'alerte est dépassé
3	Critical	Le service a un problème
4	Unknown	Impossible de connaitre l'état de service

Tableau II. 2: Signification des codes de retour

Comme nous pouvons le constater sur la figure ci-dessous, les plugins fonctionnent en effectuant des tests en local et à distance par le biais de divers moyens comme l'installation des agents NRPE ou NSClient ou autres.

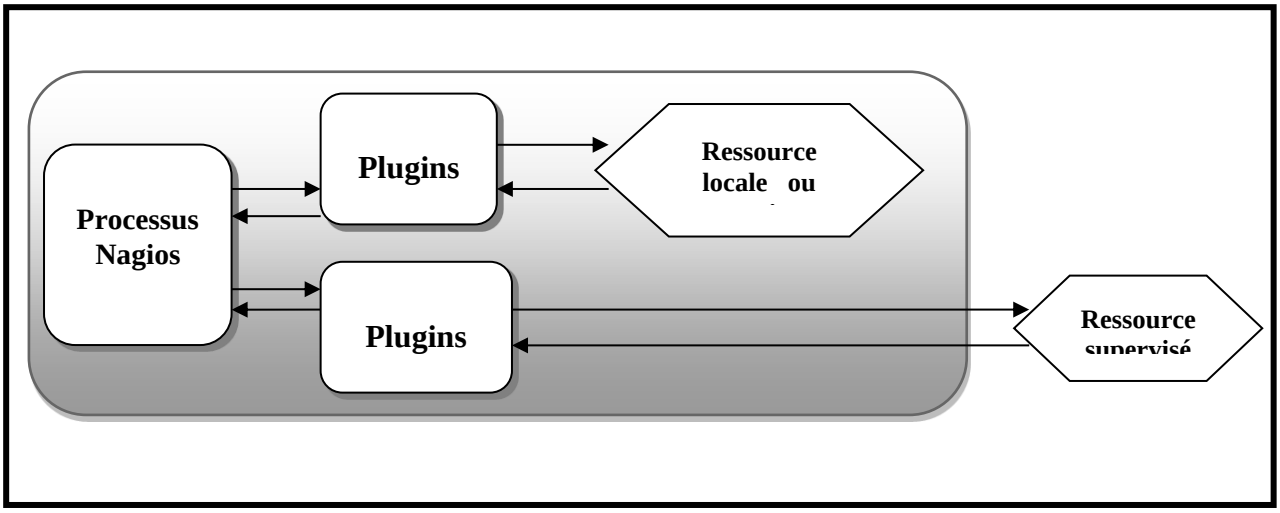

Figure II. 4: Principe du fonctionnement des plugins

III.1.4. Les fichiers de configuration

Nagios s'appuie sur différents 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** est le fichier de configuration principal de Nagios. Il contient la liste

des autres fichiers de configuration comme il comprend l'ensemble des directives globales de fonctionnement ;

- **Cgi.cfg** contient un certain nombre de directives qui affectent le mode de fonctionnement des CGI. Il s'avère qu'il joue un rôle intéressant dans la définition des préférences concernant l'interface web de Nagios ;

- **Resource.cfg** permet de définir des variables globales réutilisables dans les autres fichiers. Etant inaccessible depuis les CGI qui génèrent l'interface, ce fichier peut être utilisé pour stocker des informations sensibles de configuration ;

- **Commands.cfg** contient les définitions des commandes externes, telles que celles qui seront utiles pour la remontée d'alerte ;

- **Checkcommands.cfg** contient les définitions des commandes de vérification prédéfinies et celles définies par l'utilisateur ;

- **Hosts.cfg** définit les différents hôtes du réseau à superviser. A chaque hôte est associé un nom, une adresse IP, et un test à effectuer par défaut pour caractériser l'état de l'hôte, etc ;

- **Services.cfg** associe à chaque hôte ou à chaque groupe d'hôtes l'ensemble des services qui doivent être vérifiés ;

- **Hostsgroups.cfg** définit des groupes d'hôtes pour regrouper des hôtes selon des caractéristiques communes. Un hôte peut appartenir à plusieurs groupes ;

- **Contacts.cfg** déclare les contacts à prévenir en cas d'incident et définit les paramètres des alertes (fréquences des notifications, moyens pour contacter ces personnes, plages horaires d'envoi des alertes...).

Chapitre III

Modularisation du logiciel « Nagios »

Dans ce dernier chapitre, nous allons présenter la procédure adoptée pour superviser notre réseau Wi-Fi contrôlé par un contrôleur Wi-Fi « Ruckus ».

I. Environnement de mise en place

I.1. Environnement matériel

Nous allons installer notre logiciel sur un serveur ayant les caractéristiques suivantes :

- Système d'exploitation linux : Fedora 14 ;
- Microprocesseur dual core;
- Connexion internet.

I.2. Environnement logiciel

- La solution de supervision Nagios ;
- Les greffons de Nagios, Nagios-plugins ;
- Le plugin NDOutils pour le stockage des données de Nagios dans la base de données MySQL ;
- Le plugin NSClient pour la supervision des serveurs Windows ;
- Le plugin NRPE pour la supervision des serveurs Linux ;
- le plugin PnP4Nagios, permet de générer des graphes sur les hosts et services surveillés par Nagios ;
- le plugin ruckus zone director pour superviser le réseau Wi-Fi

II. Mise en place de Nagios

II.1. Prérequis Nagios

En plus des plugins Nagios, nous sommes appelées à satisfaire certaines dépendances. Les prérequis d'installation sont donc :

- Dépendances LAMP : Apche2, PHP5, MySQL
- Librairies Perl
- Les librairies graphiques : GD, libgd libpng, libjpeg…
- Compilateur : gcc, gcc-gc++

II.2. Installation de Nagios

Les étapes d'installation et de configuration de « Nagios » et ses plugins Nagios-plugins NDOutils seront détaillées dans l'annexe.

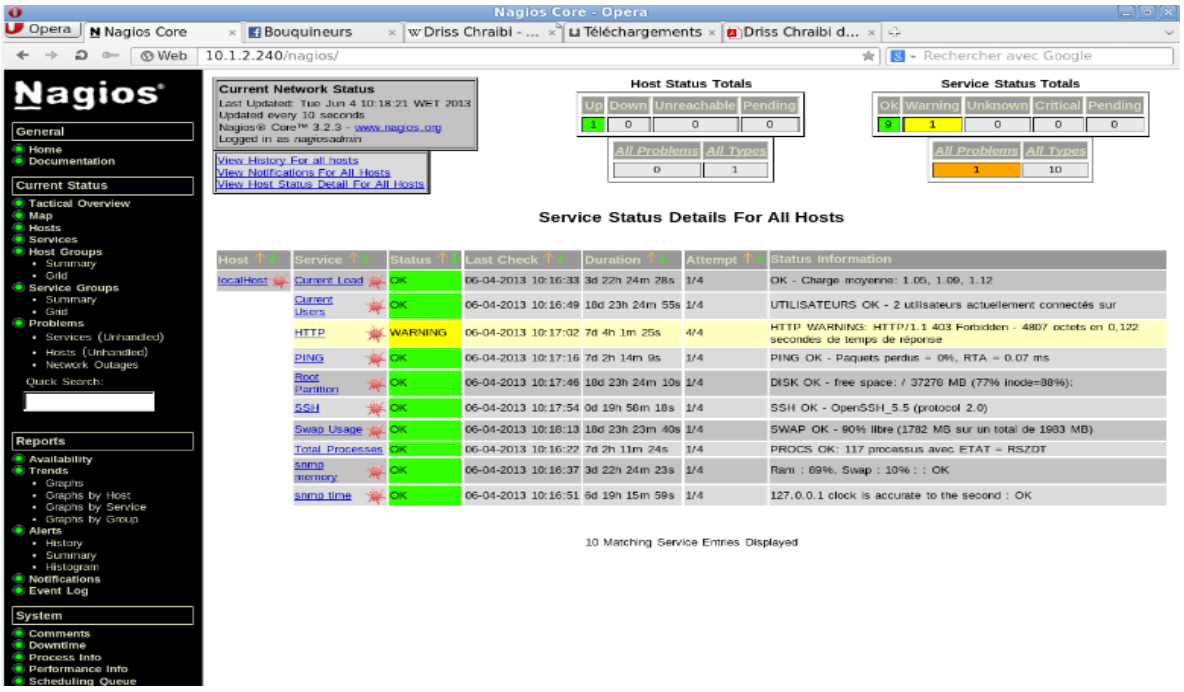

Figure III. 1 : Interface de Nagios

II.3. Installation de NSClient

Pour la supervision des serveurs Windows, nous allons installer le greffon NSClient sur la machine distante et vérifier la présence de la commande « check_nt » parmi les plugins installés de Nagios.

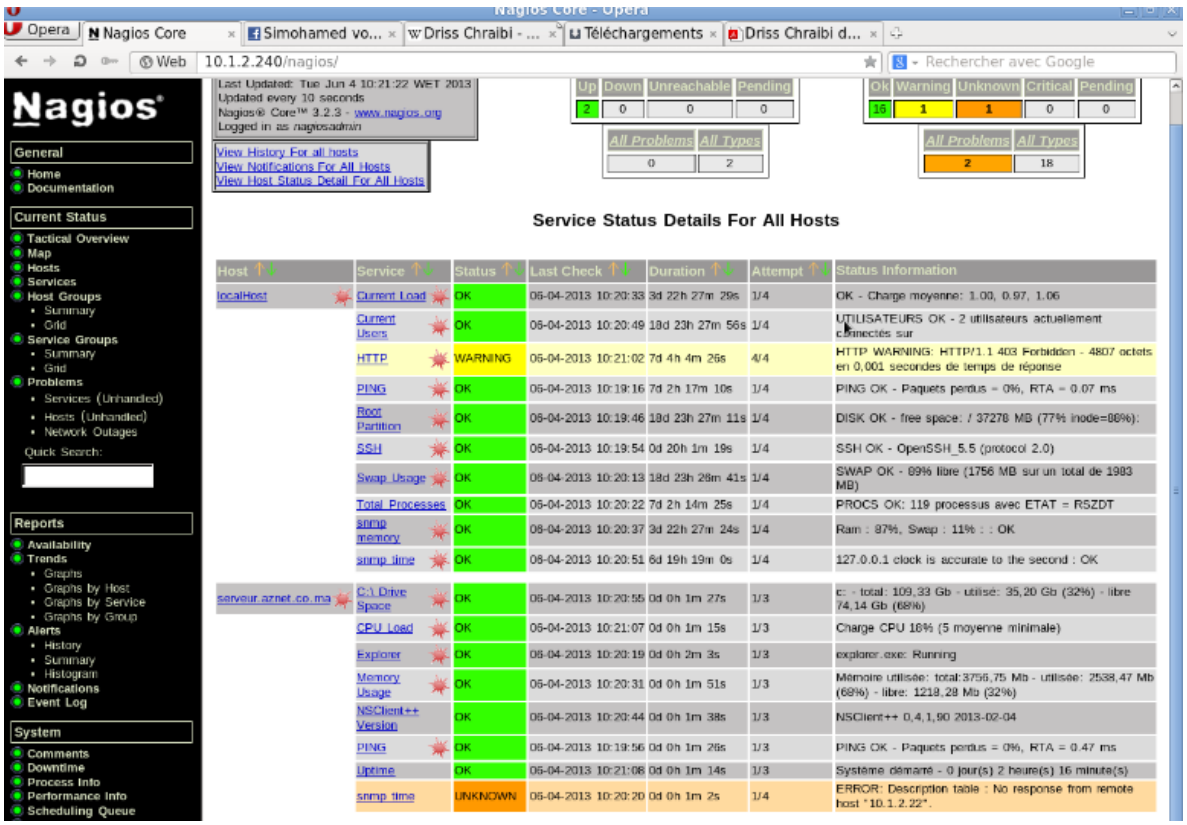

Figure III. 2 : supervision de Windows

II.4. Installation de NRPE

Pour superviser les serveurs Linux, nous allons installer le greffon « NRPE » sur la machine distante et vérifier la présence de la commande « check_nrpe » parmi les plugins installés de Nagios.

II.5. Installation PnP4Nagios

Afin d'avoir des graphes, nous avons choisit d'installer PnP4Nagios, le plugin permettant de générer des graphes sur les hosts et les services surveillés par Nagios.

Figure III. 3: Graphe associé à la supervision

III. Nagios et la supervision du réseau Wi-Fi

Afin de pouvoir superviser notre réseau Wi-Fi contrôlé par « Ruckus » nous allons dans un premier temps, télécharger le plugin check zone director.

Et ensuite, nous allons modifier le code écrit en langage de programmation « Perl » afin d'avoir une vue global sur notre réseau Wi-Fi.

Dans notre cas nous allons ajouter la fonctionnalité permettant l'affichage du nombre de point d'accès liés à notre contrôleur Wi-Fi.

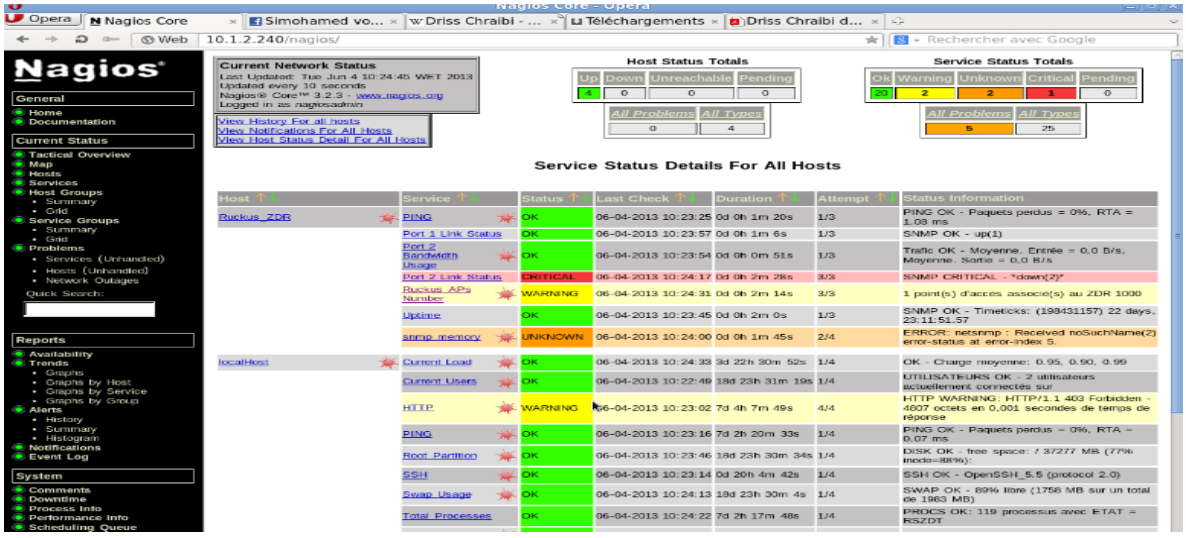

Figure III. 4 : la supervision du réseau Wi-Fi

Dans la phase suivante nous souhaitons associer notre supervision Wi-Fi au plugin

PnP4Nagios afin de générer des graphes et d'avoir une supervision en temps réel de notre Réseau Wi-Fi. Pour effectuer cette tâche nous allons associer notre plugin « check zone director » au plugin PnP, qui est un module permettant à Nagios de stocker, dans une base RRD et d'afficher via une interface Web , des données provenant des plugins Nagios , selon la procédure suivante :

PnP stocke ces templates dans deux endroits :

- /usr/local/pnp4nagios/share/templates.dist → Il s'agit des modèles inclus avec PNP ;
- /usr/local/pnp4nagios/share/templates → Il s'agit des modèles personnalisés.

Nous accédons ainsi à : /usr/local/pnp4nagios/share/templates pour créer notre propre Template qui doit respecter les conditions suivantes:

- Les modèles doivent avoir le code PHP valide.
- Les modèles ne doivent pas réaliser des sorties (echo, return, etc …).
- Les deux tableaux $opt[] et $def[] doivent y apparaître, Ces deux tableaux sont nécessaires pour l'exécution de la commande 'rrdtool graph'

Après la création de notre Template un fichier XML se génère automatiquement.

Figure III. 5 : Graphe associé à la supervision Wi-Fi

Conclusion générale

En guise de conclusion, il convient de rappeler que ce travail n'est qu'une tentative modeste d'élaboration de sécurité réseau pour l'HCEFLCD et de supervision pour l'entreprise AZ-Net. Certes, nous avons déployé des efforts énormes en vue de concrétiser ces deux projets mais concernant notre premier sujet il est important de souligner que la plateforme mise en place n'est qu'une plateforme de teste, et que nous n'avons pas pu tester toutes les fonctionnalités offertes par le produit Forefront UAG, à cause de l'insuffisance de Mémoire Vive. De même, lors de la réalisation du deuxième projet de supervision Wi-Fi, plusieurs fonctionnalités n'ont pas pu être ajoutées afin d'avoir une vue globale sur notre réseau Wi-Fi, vu la présence de la contrainte du temps.

Ce projet nous a permis d'appliquer les connaissances théoriques que nous avons acquises au cours de ces deux ans de formation au sein de la Faculté des sciences et techniques de Fès. De surcroît, il nous a permis de faire un premier pas vers l'intégration du monde professionnel, et nous a munis de l'expérience nécessaire pour la réussite d'une telle insertion. Nous avons rencontré de nombreux problèmes, auxquels nous avons tenté de trouver des solutions et des alternatives. En effet, ce projet nous a offert la chance de découvrir et d'utiliser des outils et des moyens auxquels nous n'avions pas accès auparavant.

Durant la période d'analyse des besoins nous avons fait de notre mieux pour élaborer un mini cahier de charge tiré et déduit à partir de notre étude de l'existant.

En somme, nous espérons par ce travail qui est principalement le fruit de l'aide et du soutien de nos enseignants et de nos encadrants externes. D'une part, avoir participé modestement à l'amélioration du service informatique du HCELCD, et d'autre part, avoir répondre au besoin de l'entreprise AZ-Net.

Bibliographie

Ouvrage :

- ***Mise en place du serveur UAG :***
  - Microsoft Forefront UAG 2010 Administrator's handbook
- ***Modélisation du « Nagios » pour la supervision Wi-Fi :***
  - NAGIOS au cœur de la supervision Open Source

Webographie :

- ***Mise en place d'un serveur UAG :***
  - http://danstoncloud.com/blogs/simplebydesign/archive/2010/08/23/uag-directaccess-et-le-pr-233-requis-des-deux-adresses-ip-publiques.aspx
  - http://www.isaserver.org/articles-tutorials/configuration-ecurity/Microsoft-Forefront-UAG-Configuring-Forefront-UAG-DirectAccess-Server-Part1.html
  - http://blogs.technet.com/b/stanislas/archive/2009/09/30/installation-pas-pas-d-une-plateforme-directaccess-avec-utilisation-de-forefront-uag-partie-3-configuration-de-directaccess-dans-forefront-uag.aspx
- ***Modélisation du « Nagios » pour la supervision Wi-Fi :***
  - http://blog.nicolargo.com/nagios-tutoriels-et-documentations
  - http://blog.nicolargo.com/2007/12/des-graphes-dans-nagios-avec-pnp.html
  - http://wiki.monitoring-fr.org/nagios/addons/pnp/creation-template-graph

Tables des figures

- ***Mise en place d'un serveur UAG :***

- ***Modélisation du « Nagios » pour la supervision Wi-Fi :***

Liste des Tableaux

- ***Mise en place d'un serveur UAG :***

- ***Modélisation du « Nagios » pour la supervision Wi-Fi :***

Liste des Acronymes et Abréviations

abréviation	***Signification***
UAG	Unified Access Gateway
OWA	Outlook Web Access
VPN SSL	Virtual Private Network Secure Sockets Layer
SSO	Single Sing On
PBS	Product BreackDow Structure
WBS	Work BreackDow Structure
DNS	Domaine Name Service
AD-DS	Active Directory Domain Services
NLS	Network Location Service
IIS	Internet Information Services
GPO	Group Policy Object
IPsec	IPsecurity
NRPT	Name Resolution Policy Table
NAP	Network Access Protection
CRL	Certificate Revocation List
Wi-Fi	Wirless fidelity
AAA	Authentication, Authorization, and Accounting
RADIUS	Remote Authentication Dial-In User Service
CGI	Common Gateway Interface
NRPE	Nagios Remote Plug-Ins Executor
NSClient	Nagios Service Client
GD	Gift draw
NDO	Network daemon outils
RRD	Round Robin Database
PNP	PNP is NOT Perfparse

Annexe

Après avoir téléchargé les prérequis nécessaires pour Nagios, il faut commencer l'installation. Dans un premier temps, nous commençons par la mise en place des différents Plugins.

```
# yum -y install nagios
# yum -y install nagios-plugins
#  yum  -y  install  nagios-plugins-ping  nagios-plugins-tcp
nagios-plugins-udp  nagios-plugins-http  nagios-plugins-dns
nagios-plugins-smtp  nagios-plugins-ldap  nagios-plugins-
pgsql nagios-plugins-mysql
```

Figure-Annexe 1: Installation des Plugins

Ensuite nous sommes appelées à configurer le serveur web (Apache dans notre cas). Nous devons pour cela modifier le fichier « **nagios.conf** » dans « **/etc/httpd/conf.d/** » pour autoriser l'accès depuis toutes les sources.

```
# vi /etc/httpd/conf.d/nagios.conf
> Remplacer les lignes deny from all par allow from all
```

Figure-Annexe 2: Autorisation d'Access

Nous devons également générer un couple login/password pour accéder à l'interface Web d'administration. Pour cela, il faut:

```
# htpasswd -c /etc/nagios/passwd admin
```

Figure-Annexe 3: création du login/password

Dans notre configuration nous avons passé au Fedora en mode SELINUX permissive, pour que les scripts CGI de Nagios puissent s'exécuter correctement.

```
# vi /etc/selinux/config
> SELINUX=disabled
# reboot
```

Figure-Annexe 4: configuration en mode SELINUX

Il ne reste plus qu'à vérifier que le serveur Web marche bien. Pour tester les fichiers de configuration, Il faut utiliser la commande suivante:

```
# nagios -v /etc/nagios/nagios.cfg
...
Total Warnings: 0
Total Errors: 0
Things look okay - No serious problems were detected
during the pre-flight check
```

Figure-Annexe 5: teste des fichiers de configuration

Maintenant, nous pouvons lancer le processus:

```
# service nagios start
```

Figure-Annexe 6: lancement du service Nagios

Il ne faut pas oublier de forcer le démarrage du processus au reboot de la machine grâce à la commande :

```
# chkconfig --levels 235 nagios on
```

Figure-Annexe 7: Forcement du démarrage

En cas de problème (serveur Web injoignable par exemple), il faut vérifier que le Firewall autorise bien les requêtes HTTP entrantes.

```
# iptable -A INPUT -i eth0 -p tcp -dport 80 -j ACCEPT
# /sbin/iptables-save
```

Figure-Annexe 8: règles de routage

Après avoir installé Nagios, nous pouvons passer à l'installation de PnP4Nagios

- **Installation des prérequis :**

D'abord il faut installer les librairies suivantes:

```
sudo aptitude install rrdtool librrds-perl php5-gd
```

Figure-Annexe 9: Installation des librairies

Avant l'installation nous sommes appelé à configurer une variable posant problème dans le module PHP d'apache en éditant le fichier /etc/php5/apache2/php.ini:

```
; Magic quotes for incoming GET/POST/Cookie data.
magic_quotes_gpc = Off
```

Figure-Annexe 10: Configuration du variable

Nous récupérons l'archive de la version 0.6.6 puis nous lançons la configuration:

```
wget
https://downloads.sourceforge.net/project/pnp4nagios/PNP-
0.6/pnp4nagios-0.6.6.tar.gz
tar zxvf pnp4nagios-0.6.6.tar.gz
cd pnp4nagios-0.6.6
./configure
```

Figure-Annexe 11: lancement de la configuration

Nous devons obtenir le résumé suivant:

```
General Options:
------------------------ -------------------
Nagios user/group: nagios nagios
Install directory: /usr/local/pnp4nagios
HTML Dir: /usr/local/pnp4nagios/share
Config Dir: /usr/local/pnp4nagios/etc
Location of rrdtool binary: /usr/bin/rrdtool Version 1.3.1
RRDs Perl Modules: FOUND (Version 1.3001)
RRD Files stored in: /usr/local/pnp4nagios/var/perfdata
process_perfdata.pl                                  Logfile:
/usr/local/pnp4nagios/var/perfdata.log
Perfdata        files        (NPCD)        stored        in:
/usr/local/pnp4nagios/var/spool
Web Interface Options: ------------------------ ---------
----------
HTML URL: http://localhost/pnp4nagios
Apache Config File: /etc/apache2/conf.d/pnp4nagios.conf
```

Figure-Annexe 12: résumé de la configuration

Puis, nous compilons/installons:

```
make all
sudo make install
sudo make install-webconf
sudo make install-config
sudo /etc/init.d/apache2 restart
```

Figure-Annexe 13: compilation

- **Configuration de Nagios pour prendre en compte Pnp4Nagios**

Nous commençons par éditer le fichier /usr/local/nagios/etc/nagios.cfg:

```
process_performance_data=1
service_perfdata_file=/usr/local/nagios/var/service-perfdata
service_perfdata_file_template=DATATYPE::SERVICEPERFDATAtTIME
T::$TIMET$tHOSTNA
ME::$HOSTNAME$tSERVICEDESC::$SERVICEDESC$tSERVICEPERFDATA::$S
ERVICEPERFDATA$t
SERVICECHECKCOMMAND::$SERVICECHECKCOMMAND$tHOSTSTATE::$HOSTST
ATE$tHOSTSTATETYP
E::$HOSTSTATETYPE$tSERVICESTATE::$SERVICESTATE$tSERVICESTATET
YPE::$SERVICESTAT
ETYPE$
service_perfdata_file_mode=a
service_perfdata_file_processing_interval=15
service_perfdata_file_processing_command=process-service-
perfdata-file
host_perfdata_file=/usr/local/nagios/var/host-perfdata
host_perfdata_file_template=DATATYPE::HOSTPERFDATAtTIMET::$TI
MET$tHOSTNAME::$H
OSTNAME$tHOSTPERFDATA::$HOSTPERFDATA$tHOSTCHECKCOMMAND::$HOST
CHECKCOMMAND$tHO
STSTATE::$HOSTSTATE$tHOSTSTATETYPE::$HOSTSTATETYPE$
host_perfdata_file_mode=a
host_perfdata_file_processing_interval=15
host_perfdata_file_processing_command=process-host-perfdata-
file
```

Figure-Annexe 14: fichier Nagios.cfg

Puis, nous prenons en compte le répertoire des plugins Pnp4Nagios en ajoutant la ligne suivante dans le fichier /usr/local/nagios/etc/objects/resource.cfg:

```
# Sets $USER2$ to be the path to the PNP4Nagios plugins
$USER2$=/usr/local/pnp4nagios/libexec
```

Figure-Annexe 15: path de Pnp4Nagios

Enfin, nous configurons le plugin dans le fichier /usr/local/ngs/etc/objects/commands.cfg

```
# PNP4nagios
define command{
command_name process-service-perfdata-file
command_line        $USER2$/process_perfdata.pl        --
bulk=/usr/local/nagios/var/service-perfdata
}
define command{
command_name process-host-perfdata-file
command_line        $USER2$/process_perfdata.pl        --
bulk=/usr/local/nagios/var/host-perfdata
}
```

Figure-Annexe 16: configuration du plugin

Nous relançons après Nagios pour prendre en compte la configuration:

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

Figure-Annexe 17: la relance de Nagios

- **Configuration de Pnp4Nagios**

La configuration se fait en accédant à l'URL. Le script install.php devrait être exécuté. Ce dernier effectue un check de configuration. Si tout est vert, tout est bien, sinon il existe des anomalies dans la configuration et dans ce cas, il est prudent de supprimer ce script:

```
sudo rm /usr/local/pnp4nagios/share/install.php
```

Figure-Annexe 18: suppression du script