

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Saad Dahleb Blida 1



Faculté des Sciences

Département d'Informatique

Spécialité : Sécurité des Systèmes d'Information

**Mémoire de Fin d'étude**

En vue d'obtention de Master 2 en Informatique

**Thème**

**Conception d'une architecture réseau  
d'entreprise sécurisé**

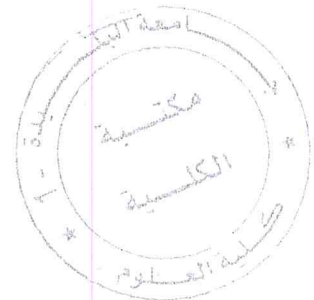
Organisme d'accueil : Groupe SAIDAL

Présenté par :

Guellati Med Abdelmalek et Mezhoud Sid Ali

Promotrice : Arkam Meriem

Encadrant : Bahiani Amine



Année Universitaire 2016/2017

MA-004-387-1

## Remerciement

*En guise de reconnaissance, je tiens à témoigner mes sincères remerciements à toutes les personnes qui ont contribués de près ou de loin au bon déroulement de mon stage de fin d'étude et à l'élaboration de ce modeste travail.*

*Mes sincères gratitudees à Mme Arkam.M pour la qualité de son enseignement, ses conseils et son intérêt incontestable qu'il porte à tous les étudiants.*

*Je tiens à remercier l'ensemble du personnel de Groupe SAIDAL pour leur patience, leurs conseils pleins de sens et pour le suivi et l'intérêt qu'ils ont portaient à mes travaux.*

*Dans l'impossibilité de citer tous les noms, nos sincères remerciements vont à tous ceux et celles, qui de près ou de loin, ont permis par leurs conseils et leurs compétences la réalisation de ce mémoire*

*Enfin, je n'oserais oublier de remercier tout le corps professoral de (votre établissement), pour le travail énorme qu'il effectue pour nous créer les conditions les plus favorables pour le déroulement de nos études.*



*Dédicaces*

*À notre raison de vivre , d'espérer,*

*À notre source de courage ,*

*À ceux qu'on a de plus chères, nos petites familles  
pour leurs sacrifices sans limite,*

*À nos enseignants pour leurs patience, leurs soutien, leurs  
encouragement ,et*

*À nos amis pour leur témoigner une amitié et fidélité  
indéfinies.*

Introduction général .....	1
<b>Chapitre I :</b>	
Introduction .....	2
1. Sécurité informatique .....	3
1.1. Objectifs de la sécurité informatique .....	3
1.2. La sécurité des Systèmes d'informations .....	3
. Vulnérabilité informatique .....	4
2.1. Criticité d'une vulnérabilité .....	4
2.2. La cause de la vulnérabilité des systèmes .....	4
2.3. Quelques systèmes les plus vulnérables .....	5
3. Les risques .....	7
3.1. Classification des risques .....	7
4. Les Attaques .....	8
4.1. Les types d'attaque .....	8
4.3. Les effets d'une attaque .....	12
5. Principaux outils de sécurité informatique .....	12
5.1. Cryptage .....	12
5.2. Authentification .....	16
5.2.1 Les protocoles d'authentification .....	16
5.3. Pare-feu (Firewall) .....	20
5.4. IDS .....	23
5.5. IPS .....	24
5.6. Honeypot .....	25
5.7. Les serveurs proxy: .....	25
5.8. L'antivirus .....	26

Conclusion.....	27
-----------------	----

## Chapitre II :

Introduction .....	28
1. Présentation de l'organisme d'accueil .....	28
1.2 Historique .....	29
1.3. Les Missions.....	29
1.4. Organigramme générale du Groupe SAIDAL.....	30
1.5. Site de production de Dar El-Beida.....	32
1.6. Lieu d'affectation du stage : la sous-direction de maintenance .....	32
2. Présentation du sujet.....	34
3. Plan général du réseau informatique de Groupe SAIDAL .....	34
4. Notre solution .....	34
4.1 Partie passerelle internet.....	35
4.1.1. Développement de la structure de l'inter-réseau .....	36
4.2. Partie Datacenter .....	40
4.2.1.L'architecture proposée.....	41
4.2.2. La Redondance .....	41
4.2.3. Sécurité Datacenter.....	42
4.3 Partie Authentification RADIUS .....	45
4.3.1. Authentification.....	45
4.3.2. Radius.....	45
4.3.3 Fonctionnement de RADIUS .....	45
4.3.4.Format des paquets.....	46
4.3.5.Protocole 802.1X.....	47
4.3.6.Le point d'accès au réseau (PAE) .....	48

4.3.7.L'architecture proposée.....	50
4.3.8.Choix du mécanisme d'Authentification .....	50
4.3.9. Fonctionnement d'PEAP.....	51
Conclusion.....	53

### **Chapitre III:**

Introduction .....	54
1. Supports et logiciel de tests.....	54
1.1 Présentation de GNS3 .....	54
1.2 Présentation de VMware Workstation .....	55
2. Les configurations mise en place .....	56
2.1. Partie passerelle internet.....	56
2.1.1. Présentation de l'architecture.....	56
2.1.2. L'adressage.....	57
2.1.3. Les configurations .....	58
2.2. Partie Datacenter .....	60
2.2.1. Présentation de l'architecture.....	60
2.2.2. L'adressage.....	61
2.2.3. Les configurations .....	62
2.3. La partie Authentification RADIUS .....	63
2.3.1. Les configurations .....	63
3. Test sur le réseau .....	66
3.1. TEST de VPN entre site Groupe SAIDAL et site de Blida: .....	66
3.2 Test de VPN Remote Access .....	68
3.3 Test de NAT .....	71

3.4. Test de Redondance .....	71
3.4.1. Cas où il y a pas une panne .....	71
3.4.2. Cas de panne de switch ESW1 .....	72
3.4.3. cas de panne du parefeu ASA-1 .....	72
3.5. Test de sécurité de protocole hsrp: .....	73
3.5.1. Cas ou HSRP n'est pas sécurisé : .....	73
Conclusion.....	75
Conclusion général.....	76

## Les Figures

### Chapitre I

Figure I.1 : le nombre de vulnérabilités de sécurité entre 2009 et 2014.....	05
Figure I.2 : le nombre de vulnérabilités trouve en 2013 pour certains vendeurs connus .....	06
Figure I.3 : le nombre de vulnérabilités trouve en 2013 pour certain application connus.....	07
Figure I.4:le nombre de vulnérabilités en 2013 pour certain système d'exploitation .....	10
Figure I.5 : schéma de l'attaque ARP Spoofing.....	11
Figure I.6 : Table ARP du client avant attaque.....	11
Figure I.7 : Table ARP après attaque.....	09
Figure I.8 : les deux modes de fonctionnement 'IPSec.....	16
Figure I.9 : authentification du protocole PAP.....	17
Figure I.10 : authentification du protocole CHAP.....	18
Figure I.11 : authentification du protocole MS-CHAP.....	19
Chapitre II :	
Figure II.01 : Organigramme générale du Groupe SAIDAL .....	31
Figure II.02 : Organigramme de service de la maintenance.....	33
Figure II.03 : Décomposition d'un service .....	33
Figure II.04: plan initial de réseau de Groupe SAIDAL.....	34
Figure II.05 : plan générale de réseau de Groupe SAIDAL.....	35
Figure II.06 : Architecture de la solution proposée (partie passerelle Internet) .....	35

Figure II.07 : Architecture de la solution proposée (partie Data Center) .....	41
Figure II.08 : Organigramme du fonctionnement RADIUS .....	46
Figure II.09 : Format d'un paquet RADIUS .....	47
Figure II.10 : Architecture d'authentification 802.1X .....	48
Figure II.11 : Les trois entités qui interagissent dans 802.1X.....	48
Figure II.12 : La structure d'un port dans 802.1x (PAE) .....	49
Figure II.13 : Architecture du réseau interne (partie utilisateurs).....	50
Figure II.14 : Diagramme d'échanges PEAP .....	51
<b>Chapitre III :</b>	
Figure III.01 Interface graphique de l'émulateur GNS3.....	55
Figure III.02 : Interface de VMware Workstation .....	55
Figure III.03 : l'architecture proposée (partie passerelle Internet) .....	56
Figure III.04: les propriétés de mise en cache d'ISA Server .....	59
Figure III .05 : le filtrage url dans ISA Server.....	59
Figure III.06 : les propriétés de blacklistURL dans ISA Server.....	60
Figure III.07 : l'architecture proposée (partie Data Center .....	61
Figure III.08: l'architecture du réseau interne LAN .....	63
Figure III.09 : Comptabilisation NPS .....	65
Figure III.10 : Test de connectivité depuis le Site Groupe SAIDAL vers le site Blida .....	67
Figure III.11 : Test de connectivité depuis le site Blida vers le site Groupe SAIDAL .....	67
Figure III.12 : Etat du tunnel VPN site to site.....	68
Figure III.13 : test de VPN Access .....	69
Figure III.14 : test de VPN Access .....	69
Figure III.15 : état de VPN .....	70
Figure III.16 : Configuration de Parfeu ASA1 .....	70
Figure III.17 : Test de NAT.....	71
Figure III.18 : L'état du Protocole HSRP pour le switch ESW1.....	71
Figure III.19 : L'état du Protocole GLBP pour le switch S2 .....	71
Figure III.20 : L'état du Protocole failover pour le parfeu ASA-1 .....	72
Figure III.21 : L'état du Protocole failover pour le parfeu ASA-2 .....	72



Figure III.22 : L'état du Protocole HSRP pour le switch ESW2.....	72
Figure III.23 : L'état de parfeu ASA-2.....	73
Figure III.24 : L'état du Protocole HSRP pour le switch ESW1.....	73
Figure III.25 : L'état du Protocole HSRP pour le switch ESW2.....	73
Figure III.26:Attaque HSRP .....	74
Figure III.27:Résultat de l'Attaque HSRP.....	74

## Liste des Tableaux

### Chapitre I :

Tableau I.1 : criticité d'une vulnérabilité.....	04
Tableau I.2 : les types d'authentification en utilisant EAP.....	21
Tableau I.3: les plages des ACLs et leurs types.....	22

### Chapitre II :

Tableau II.01: Eléments d'un message RADIUS.....	47
--	----

### Chapitre III :

Tableau III.01 : le plan d'adressage des sites de Groupe SAIDAL et de Blida.....	56
Tableau III.02 : l'adressage des sites de Groupe SAIDAL et de Blida.....	57
Tableau III.03 : le plan d'adressage des vlans (partie Data Center) .....	61
Tableau III.04 : l'adressage des vlans (partie Data Center).....	62

## Bibliographie

### Chapitre I :

- [1] <http://www.hapsis.fr/index.php/blog/item/333-comment-gerer-les-vulnerabilites-informatiques-de-son-entreprise>
- [2] [http://xenod.free.fr/0\\_La\\_securite\\_informatique.htm#Introduction](http://xenod.free.fr/0_La_securite_informatique.htm#Introduction)
- [3] <http://www.developpez.com/actu/67200/>
- [4] <http://www.net-gestion.fr/PBCPPlayer.asp?ID=1385774>
- [5] [http://www.info-virus.com/comprendre\\_les\\_virus\\_informatiqu.htm](http://www.info-virus.com/comprendre_les_virus_informatiqu.htm)
- [6] <http://www.inetdoc.net/guides/tutoriel-secu/tutoriel.securite.attaquesprotocoles.dhcp.html>
- [7] [http://sid.rstack.org/static/articles/j/o/u/Jouer\\_avec\\_le\\_protocole\\_ARP\\_dadb.html](http://sid.rstack.org/static/articles/j/o/u/Jouer_avec_le_protocole_ARP_dadb.html)
- [8] <http://www.it-connect.fr/attaque-man-in-the-middle-et-dos-via-arp-spoofing/>
- [9] <http://www.frameip.com/ipsec/>

- [10] [http://livre.g6.asso.fr/index.php?title=Echanges\\_ISAKMP/IKEv1](http://livre.g6.asso.fr/index.php?title=Echanges_ISAKMP/IKEv1)
- [11] <https://msdn.microsoft.com/fr-fr/library/cc737807%28v=ws.10%29.aspx>
- [12] <https://msdn.microsoft.com/fr-fr/library/cc757631%28v=ws.10%29.aspx>
- [13] <https://technet.microsoft.com/fr-fr/library/cc731462%28v=ws.10%29.aspx>
- [14] [https://www.juniper.net/techpubs/software/aaa\\_802/sbrc/sbrc70/sw-sbrc-admin/html/EAP-029.html](https://www.juniper.net/techpubs/software/aaa_802/sbrc/sbrc70/sw-sbrc-admin/html/EAP-029.html)
- [15] <https://www.ciscomadesimple.be/2011/11/30/access-list-reflexive/>
- [16] [http://www.cisco.com/c/en/us/td/docs/ios/12\\_2/security/configuration/guide/fsecur\\_c/scflock.html](http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scflock.html)
- [17] <http://www.cisco.com/c/en/us/support/docs/security/ios-firewall/13814-32.html>
- [18] [http://igm.univ-mlv.fr/~dr/XPOSE2009/Sonde\\_de\\_securite\\_IDS\\_IPS/IDS.html](http://igm.univ-mlv.fr/~dr/XPOSE2009/Sonde_de_securite_IDS_IPS/IDS.html)
- [19] <http://igm.univ-mlv.fr/~dr/XPOSE2009/botnets/honeypot.html>
- [20] <http://windows.microsoft.com/fr-fr/windows-vista/what-is-a-proxy-server>

### **Chapitre III :**

- [21] <http://mi.cnrs-orleans.fr/Security/Win2k/ISA/Presentation/isatecov.htm>
- [22] <http://www.faqxp.com/f/558.asp>
- [23] [http://www.academia.edu/5501105/Cisco\\_les\\_acl\\_cours](http://www.academia.edu/5501105/Cisco_les_acl_cours)

# Introduction général

### **Introduction générale**

Avec le développement de l'utilisation d'internet, de plus en plus d'entreprises ouvrent leurs systèmes d'information à leurs partenaires ou leurs fournisseurs, il est donc essentiel de connaître les ressources de l'entreprise à protéger et de maîtriser le contrôle d'accès et les droits des utilisateurs du système d'information.

Si une entreprise par exemple, ne prend pas de précautions, son système d'information sera en sous-entendu, sujet aux vulnérabilités et par conséquent aux attaques et exploits pouvant soit émaner de l'intérieur ou de l'extérieur par rapport à l'entreprise, ce qui serait plus que dommageable pour cette dernière dont l'un des objectifs principaux est de sécuriser son réseau.

L'objectif de notre projet est de proposer une solution qui comprendra une architecture et une stratégie sécuritaire nouvelles adaptées au besoin de l'entreprise **Groupe SAIDAL**.

Ce travail est organisé en Trois chapitres :

Le premier chapitre s'intitule "**Généralités sur la sécurité informatiques**", nous décrivons des notions de base sur la sécurité informatique et présentons quelques définitions fondamentales que nous avons jugées utiles pour avancer dans le travail.

Le second chapitre, **étude de l'existence** présente la société **Groupe SAIDAL**, son organisation et ses besoins en termes de sécurité, **Conception** qui constitue dans le même chapitre, où nous mettons une solution en adéquation avec les objectifs fixés .

Enfin, nous évoquerons la mise en place de la solution choisie dans le dernier chapitre intitulée **Test et réalisation**.

# Chapitre I

### **Introduction**

La sécurité des systèmes d'information demeure un défi permanent pour les organisations. Bien que beaucoup d'entre elles aient découvert l'importance de l'information pertinente, cruciale, encore peu parviennent à être efficaces dans la sécurisation des données en évitant les accès non autorisés, les dénis de service ou en limitant la divulgation non autorisée de l'information. De plus les avancées technologiques stimulent une plus grande utilisation des systèmes informatiques distribués qui manipulent des masses de données gérées dans des bases et des entrepôts de données mais aussi des informations provenant du Web à travers des applications 'grand public'. Ces nouveaux environnements collaboratifs doivent donc répondre à des exigences de sécurité critiques de manière à prouver que les composants logiciels ayant en charge la sécurité des SI réagissent aux différentes attaques potentielles et offrent une protection efficace de la vie privée en conformité avec les politiques de sécurité et les lois de protection sur les données personnelles.

Bien que la protection de l'information ait toujours été une préoccupation majeure des organisations, la numérisation, la dématérialisation des échanges, l'ouverture de l'accès de l'entreprise sur internet ont grandement augmenté les menaces et les vulnérabilités de l'information. La sécurité des SI est devenue un problème critique et donc stratégique dans les organisations.

Beaucoup d'organisations publiques ou privées dépendent de la fiabilité, disponibilité et de la confidentialité de leurs informations. Pour cela nous allons essayer de mettre en évidence dans ce chapitre toutes les notions de base concernant les systèmes d'informations, leurs vulnérabilités et leurs sécurisations.

### 1. Sécurité informatique

La sécurité informatique est l'ensemble des techniques qui assurent que les ressources du système d'information (matérielles ou logicielles) d'une organisation sont utilisées uniquement dans le cadre où il est prévu qu'elles le soient.

- Les systèmes informatiques sont au cœur des systèmes d'information
- Ils sont devenus la cible de ceux qui convoitent l'information
- Assurer la sécurité de l'information implique l'assurance la sécurité des systèmes informatiques
- La sécurité informatique est la science qui permet de s'assurer que celui qui consulte ou modifie des données du système en a l'autorisation

#### 1.1. Objectifs de la sécurité informatique

La sécurité informatique vise généralement cinq principaux objectifs :

- a. Authentification:** vérifier l'identité des personnes qui veulent manipuler l'information
- b. Confidentialité:** L'information ne peut être connue que par les personnes autorisées
- c. Disponibilité :** L'information doit être utilisable à la demande
- d. Intégrité :** L'information ne doit pas être altérée ou détruite par accident ou malveillance
- e. Non répudiation :** L'absence de possibilité de contestation d'une action une fois celle-ci est effectuée

#### 1.2. La sécurité des Systèmes d'informations

Un système d'Information (noté SI) représente l'ensemble des moyens nécessaires à l'élaboration, au traitement, au stockage, à l'acheminement et à l'exploitation des informations

La sécurité du système d'information est l'ensemble de mesures de sécurité physique, logique, administrative et de mesures d'urgence mises en place dans une organisation, en vue d'assurer:

- La confidentialité et l'intégrité des données de son système d'information.
- La protection de ses biens informatiques.

- La continuité de service.

## . Vulnérabilité informatique

Une vulnérabilité ou faille est une faiblesse dans un système informatique pouvant être utilisé pour obtenir un niveau d'accès illicite à une ressource d'informations ou des privilèges supérieurs à ceux considérés comme normaux pour cette ressource.

La vulnérabilité caractérise les composants du système (matériel, logiciel, les règles, les procédures, personnel) susceptibles d'être attaquées avec succès, elle est exploitée par une menace pour causer une perte. [1]

### 2.1. Criticité d'une vulnérabilité

Les modèles de criticité d'une vulnérabilité :

<b>Critique</b>	Problème critique permettant rapidement prendre le contrôle du système
<b>Important</b>	Problème pouvant être la cause d'une intrusion, mais difficilement exploitable
<b>Moyen</b>	Problème pouvant être indirectement la source d'une intrusion
<b>Mineur</b>	Problème sans conséquence directe pour la sécurité du système mais pouvant fournir des informations techniques.

Tableau I.1 : Criticité d'une vulnérabilité

### 2.2. La cause de la vulnérabilité des systèmes

Les systèmes informatiques sont vulnérables pour les raisons suivantes :

- a. La sécurité est chère et difficile. Les organisations n'ont pas de budget pour ça.
- b. La sécurité ne peut être sûre à 100%, elle est même souvent inefficace.
- c. La politique de sécurité est complexe et basée sur des jugements humains.
- d. Les organisations acceptent de courir le risque, la sécurité n'est pas une priorité.
- e. De nouvelles technologies (et donc vulnérabilités) émergent en permanence
- f. Les systèmes de sécurité sont faits, gérés et configurés par des hommes.
- g. Il n'existe pas d'infrastructure pour les clefs et autres éléments de cryptographie.



- h. L'état interdit la cryptographie dans certains cas (exportation, par exemple) dans certains pays, ce qui empêche le cryptage systématique au niveau du système d'exploitation. [2]

### 2.3. Quelques systèmes les plus vulnérables

GFI Labs (laboratoire d'innovation du Groupe Informatique) vient de publier un rapport sur les menaces de sécurité en 2014, afin de prévoir les susceptibles problèmes de sécurité qui pourrait arriver dans les années a venir.

Après analyse des chiffres du National Vulnerability Database (NVD), GFI Labs estime qu'en 2014, les chercheurs en sécurité ont découvert en moyenne 19 nouvelles vulnérabilités par jour. Un total de 7038 failles de sécurité ont été signalées en 2014, dont le tiers a été marqué comme « critiques ». Ce chiffre représente le plus élevé enregistré au cours des cinq dernières années. [3]

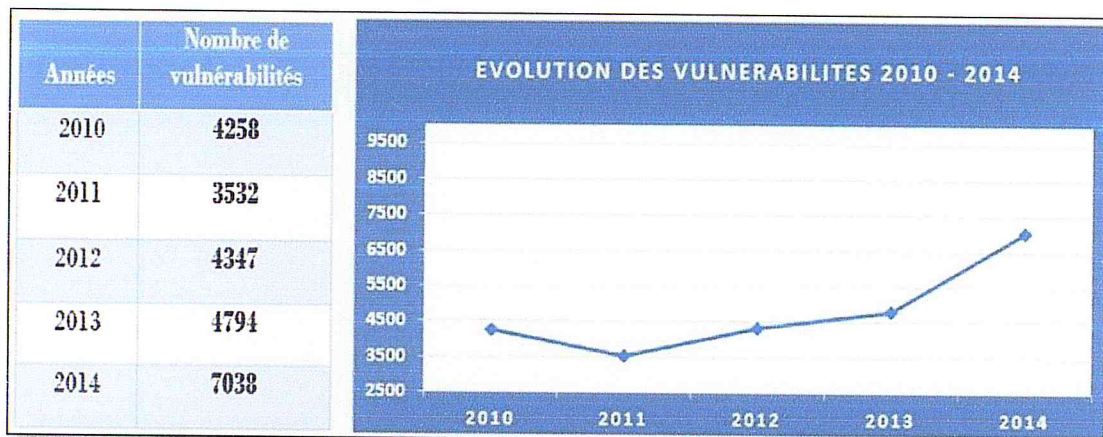


Figure I.1 : le nombre de vulnérabilité entre 2010 et 2014.

Le rapport de GFI Labs ressort également les applications, systèmes d'exploitation dont les produits ont enregistré le plus de signalisations de failles de sécurité au cours de l'année 2014.

En ce qui concerne les applications, Internet Explorer enregistre le plus de vulnérabilités critiques (220). Le navigateur est suivi par Mozilla et Chrome respectivement (57 et 86 failles critiques découvertes)

Applications	Nombre total de vulnérabilités	Vulnérabilités CRITIQUES	Vulnérabilités MAJEURES	Vulnérabilités MINEURES
Microsoft Internet Explorer	242	220	22	0
Google Chrome	124	86	38	0
Mozilla Firefox	117	57	57	3
Adobe Flash Player	76	65	11	0
Oracle Java	104	50	46	8
Mozilla Thunderbird	66	36	29	1
Mozilla Firefox ESR	61	35	25	1
Adobe Air	45	38	7	0
Apple TV	86	29	49	8
Adobe Reader	44	37	7	0
Adobe Acrobat	43	35	8	0
Mozilla Seamonkey	63	28	34	1

Figure I.3 : le nombre de vulnérabilité trouvé en 2014 pour certain application connu.

L'année dernière 24% de ces vulnérabilités ont été jugées sérieuses, soit 1887 contre 1492 l'année précédente. Selon GFI, les applications seraient responsables pour 83% de ces failles de sécurité contre 13% pour les systèmes d'exploitation eux-mêmes et 4% pour le matériel.

C'est OS X qui se trouve en pôle position des systèmes vulnérables avec 147 mentions saisies au sein de la base de données dont 64 jugées importantes. En seconde place, nous retrouvons iOS avec 127 failles devant le kernel de Linux. « Bien que les systèmes de Microsoft ont toujours un nombre considérable de vulnérabilités, il est intéressant de noter qu'ils ne sont plus dans le top 3 », affirme GFI. Reste que combinés, Windows Server 2008 et 2013 ainsi que Windows Vista, 7, 8, 8.1 et RT détiennent au total 4010 failles rapportées dont 168 importantes.

Systèmes d'exploitation	Nombre Total de vulnérabilités	Vulnérabilités CRITIQUES	Vulnérabilités MAJEURES	Vulnérabilités MINEURES
Apple Mac OS X	147	64	67	16
Apple iOS	127	32	72	23
Linux Kernel	119	24	74	21
Microsoft Windows Server 2008	38	26	12	0
Microsoft Windows 7	36	25	11	0
Microsoft Windows Server 2012	38	24	14	0
Microsoft Windows 8	36	24	12	0
Microsoft Windows 8.1	36	24	12	0
Microsoft Windows Vista	34	23	11	0
Microsoft Windows RT	30	22	8	0

Figure I.4 : le nombre de vulnérabilité en 2014 pour certain système d'exploitation

### 3. Les risques

Face aux différentes vulnérabilités susceptibles d'être exploitées pour attaquer les systèmes d'information et aux menaces multiformes existantes, il est clair que tout système d'information peut être impacté par des risques. Un risque est un événement susceptible de se produire.

#### 3.1. Classification des risques

- **Les risques Humains**

Les risques humains sont les plus importants, ils concernent les utilisateurs mais également les informaticiens.

**Malveillances:** Certains utilisateurs peuvent volontairement mettre en danger le système d'information en y introduisant en connaissance de causes des virus, ou en introduisant

Volontairement de mauvaises informations dans une base de données

**Inconscience:** De nombreux utilisateurs d'outils informatiques sont encore inconscients ou ignorants des risques qu'ils encourent aux systèmes qu'ils utilisent, et introduisent souvent des programmes malveillants sans le savoir.

- **Les risques Techniques**

**Accidents:** il s'agit là d'un évènement perturbant les flux de données en l'absence de dommages aux équipements (panne, incendie, dégâts des eaux d'un serveur ou centre informatique,..).

**Erreurs :** que ce soit une erreur de conception, de programmation de paramétrage ou de manipulation de données ou de leurs supports, l'erreur désigne les préjudices consécutifs à une intervention humaine dans le processus de traitement automatisé des données. [4]

### 4. Les Attaques

Une attaque est une activité malveillante qui consiste à exploiter une faille d'un système informatique (serveurs, routeurs, système d'exploitation, logiciel, etc.) à des fins non connues par les responsables du système et généralement préjudiciables pour le système d'information en général. Une attaque est une action qui compromet la sécurité de l'information possédée par une organisation.

#### 4.1. Les types d'attaque

- **Les attaques d'accès**

**Ingénierie sociale :** L'attaquant établit des relations avec le personnel pour obtenir des informations sur les mots de passe, La topologie du réseau,

**Portes dérobées (backdoors) :** Une porte dérobée n'est pas un programme, mais une fonctionnalité d'un programme permettant de donner un accès secret au système. Ce genre de fonctionnalité est souvent ajouté à un logiciel par l'éditeur, afin de lui permettre de surveiller l'activité du logiciel, ou de prendre le contrôle en cas de sollicitation. Généralement, les pirates informatiques une fois entrés dans le système, créent une porte dérobée afin de pouvoir y avoir accès à n'importe quel moment .

**Sniffing :** L'attaquant se met à l'écoute sur le réseau pour obtenir des informations.

- **Les attaques de modification**

- **Virus:** un programme malveillant caché dans un autre qui peut s'exécuter et se reproduire en infectant d'autres programmes ou d'autres ordinateurs [5]

- **Ver:** un programme malveillant qui peut s'auto-reproduire et se déplacer à travers un réseau en utilisant les mécanismes réseau comme internet, sans avoir réellement besoin d'un support physique ou logique (disque dur, fichier, etc.)
- **Bombe logique:** un programme malveillant qui se déclenche à une date ou à un instant donnée
- **cheval de Troie:** Un cheval de Troie est un programme d'apparence légitime conçu pour exécuter de façon cachée des actions à l'insu de l'utilisateur. En général, un cheval de Troie tente d'utiliser les droits appartenant à son environnement pour détourner, diffuser ou détruire des informations, ou encore pour ouvrir une porte dérobée qui permet à un attaquant de prendre, à distance, le contrôle de l'ordinateur
- **Les attaques par saturation (dédi de service):**
  - **DHCP Flooding:**

Le principe de cette attaque est de Consommer toutes les adresses IP disponibles de serveur

DHCP pour empêcher les autres utilisateurs de se connecter :

Le pirate simule des paquets DHCP Discover avec un identifiant changeant à chaque fois, le serveur DHCP réserve donc une IP à chaque requête. Lorsque la réserve d'adresses IP est épuisée, plus aucune nouvelle machine ne pourra se connecter au réseau. [6]
  - **Le smurf:** S'appuie sur le Ping et les serveurs de broadcast. On falsifie d'abord son adresse IP pour se faire passer pour la machine cible.
  - Les attaques de répudiation
  - **L'attaque Mac spoofing:**

Une trame Ethernet dispose d'un champ source et d'un champ destination. Ces champs sont examinés par les commutateurs Ethernet pour, d'une part, choisir sur quel port ils vont envoyer une trame reçue par examen de l'adresse MAC destination, et d'autre part mettre à jour une table associant ses ports aux adresses MAC des différents postes par examen de l'adresse MAC source. Cette table, appelée table CAM (Content Adressable Memory) dans la terminologie Cisco, contient pour chaque port les adresses MAC des hôtes qui y sont connectés.

Le contenu de cette table est mis à jour dynamiquement pour permettre le changement de port d'un hôte par exemple. [7]

L'usurpation d'adresse MAC vise à se servir de ce mécanisme de mise à jour pour forcer le commutateur à croire que la station dont nous voulons écouter le trafic se trouve sur notre port. Le principe est simple : nous envoyons une trame ayant pour adresse source l'adresse MAC de notre victime, et pour destination notre adresse MAC. Le commutateur, en recevant cette trame, met sa table à jour en associant l'adresse MAC de la victime à notre port. Dès lors, l'intégralité du trafic qui lui est destiné est dirigée sur notre port et il ne nous reste plus qu'à le lire tranquillement.

Certains commutateurs réagissent mal à de nombreux conflits d'adresse MAC en passant en mode répéteur, se conduisant alors comme des hubs.

### ➤ L'attaque ARP SPOOFING

Le principe est d'envoyer des informations à un systèmes afin de lui faire enregistrer des informations qui ne sont pas les bonnes et qui usurpent l'identité (la relation IP-MAC) d'un autre système. Partons du schéma suivant :

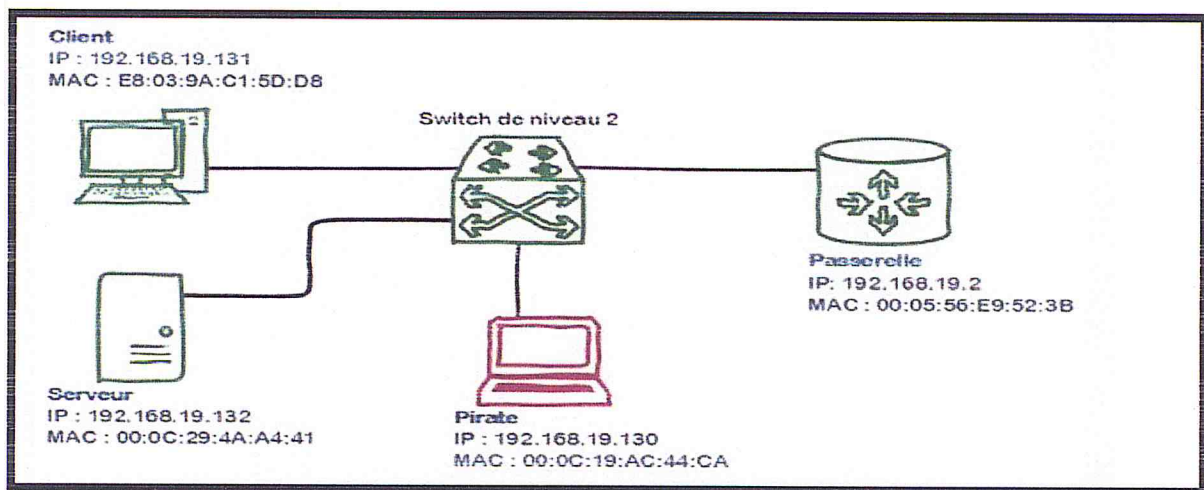
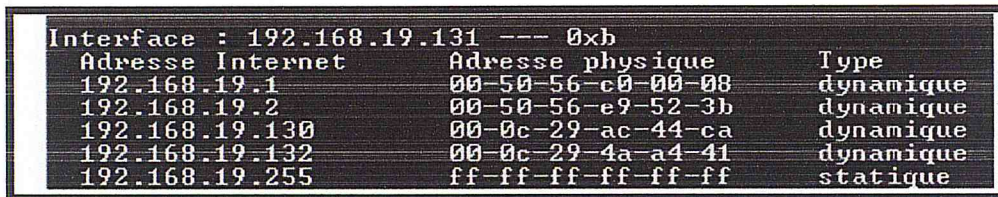


Figure I.5 : schéma de l'attaque arp spoofing

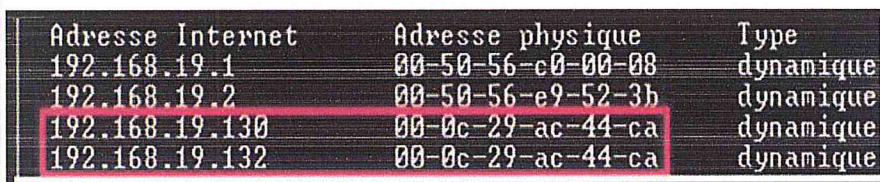
Le Pirate à l'adresse MAC **00:0C:19:AC:44:CA** et le serveur l'adresse MAC **00:0C:29:4A:A4:41**, la table adresse MAC chez le client ressemble donc à cela



Interface	Adresse Internet	Adresse physique	Type
	192.168.19.1	00-50-56-c0-00-08	dynamique
	192.168.19.2	00-50-56-e9-52-3b	dynamique
	192.168.19.130	00-0c-29-ac-44-ca	dynamique
	192.168.19.132	00-0c-29-4a-a4-41	dynamique
	192.168.19.255	ff-ff-ff-ff-ff-ff	statique

Figure I.6 : Table ARP du client avant attaque

Si le pirate envoie des paquets au client avec l'adresse IP du source du serveur mais en laissant son adresse MAC (ce qui est faisable si on construit nos paquets nous même plutôt que si on laisse notre carte réseau le faire), la table ARP de notre client va donc enregistrer le couple suivant :



Adresse Internet	Adresse physique	Type
192.168.19.1	00-50-56-c0-00-08	dynamique
192.168.19.2	00-50-56-e9-52-3b	dynamique
192.168.19.130	00-0c-29-ac-44-ca	dynamique
192.168.19.132	00-0c-29-ac-44-ca	dynamique

Figure I.7 : Table ARP après attaque

Cela vient du fait que l'enregistrement est marqué comme dynamique, donc volatile, et qu'il peut être mis à jour à chaque réception de paquet présentant des couples IP – MAC différents. Les paquets que le client va générer à destination du serveur vont donc à présent se former avec l'adresse IP destination du serveur mais l'adresse MAC destination du pirate étant donné qu'il se base pour cela sur sa table ARP et que celle-ci est falsifiée. [8]

On voit donc que si la table ARP de notre cible est falsifiée, il va former ces trames avec l'adresse IP du serveur mais va en fin de compte les envoyer au pirate car il formera ses requêtes avec comme adresse MAC de destination celle du pirate.

### Technique d'attaques par messagerie

**Le Pourriel (Spam) :** Un courrier électronique non sollicité, la plus part du temps de la publicité. Ils encombrant le réseau.

- **L'Hameçonnage(phishing):** Le phishing est une technique dans laquelle des bandes organisées de cybercriminels se font passer pour des organismes financiers ou grandes sociétés en envoyant des emails ou des pages web frauduleux pour

recupérer des mots de passe de comptes bancaires ou numéros de cartes de crédit pour détourner des fonds. Le phénomène existe depuis 1996 et a connu une accélération significative début 2003.

- **Attaques sur les mots de passe**

Les attaques sur les mots de passe peuvent consister à faire de nombreux essais jusqu'à trouver le bon mot de passe.

Dans ce cadre, notons les deux méthodes suivantes :

- **L'attaque par dictionnaire:** le mot testé est pris dans une liste prédéfinie contenant les mots de passe les plus courants.
- **L'attaque par force brute:** toutes les possibilités sont faites dans l'ordre jusqu'à trouver la bonne solution.

### 4.3. Les effets d'une attaque

- **Attaque passive :** c'est la moins dangereuse, Ne modifie pas l'information son objectif est la consultation de l'information.
- **Attaque active :** ce type d'attaque est dangereux permet de Modifier l'état d'une information, d'un serveur ou d'une communication.

## 5. Principaux outils de sécurité informatique

### 5.1. Cryptage

- ✓ **chiffrement symétrique :** la clé de chiffrement, est identique à la clé de déchiffrement : DES, IDEA
- ✓ **chiffrement asymétrique:** Une clé est utilisée pour le chiffrement et l'autre pour le déchiffrement, La clé de déchiffrement aussi appelée clé privée est normalement gardée secrète tandis que la clé de chiffrement aussi appelée clé publique est la plupart du temps distribuée.
- ✓ **SSL (Secure Socket Layer)**



La Technologie SSL est utilisée pour sécuriser la transmission de données sur Internet: elle chiffre et protège les données transmises à l'aide du protocole HTTPS. Le SSL garantit aux visiteurs de site web que leurs données ne seront pas interceptées de manière frauduleuse.

- ✓ **SSH (Secure Shell)** C'est un protocole qui permet de faire des connexions sécurisées entre un serveur et un client SSH.
- ✓ **VPN:** Les réseaux privés virtuel sont utilisés pour permettre la transmission sécurisée de données, voix et vidéo entre deux sites. Un réseau Vpn repose sur un protocole appelé "protocole de tunneling". Ce protocole permet de faire circuler les informations de l'entreprise de façon cryptée d'un bout à l'autre du tunnel pour assurer la confidentialité des données transmises entre les deux sites. Ainsi, les utilisateurs ont l'impression de se connecter directement sur le réseau de leur entreprise

### ❖ **Le protocole Ipvsec:**

IPsec est un protocole qui vise à sécuriser l'échange de données au niveau de la couche réseau. Le réseau Ipv4 étant largement déployé et la migration vers Ipv6 étant inévitable, mais néanmoins longue, il est apparu intéressant de développer des techniques de protection des données communes à Ipv4 et Ipv6. Ces mécanismes sont couramment désignés par le terme Ipvsec pour (IP Security Protocols). Ipvsec est basé sur deux mécanismes. Le premier, AH, pour Authentication Header vise à assurer l'intégrité et l'authenticité des datagrammes IP. Il ne fournit par contre aucune confidentialité : les données fournies et transmises par ce "protocole" ne sont pas encodées. Le second, Esp, pour Encapsulating Security Payload peut aussi permettre l'authentification des données mais est principalement utilisé pour le cryptage des informations. Bien qu'indépendants ces deux mécanismes sont presque toujours utilisés conjointement. Enfin, le protocole Ike permet de gérer les échanges ou les associations entre protocoles de sécurité. [09]

### ❖ **Les protocoles à base IP sec:**

#### ➤ **AH (authentication header) :**

AH est le premier et le plus simple des protocoles de protection des données qui font partie de la spécification Ipvsec Il a pour vocation de garantir :

- **L'authentification** : les datagrammes IP reçus ont effectivement été émis par l'hôte dont l'adresse IP est indiquée comme adresse source dans les en-têtes.
- **L'unicité**: un datagramme ayant été émis légitimement et enregistré par un attaquant ne peut pas être réutilisé par ce dernier, les attaques par rejeu sont ainsi évitées. .
- **L'intégrité** : un on s'assure que les champs du datagramme IP n'ont pas été modifiés pendant la transmission, dans l'entête IP qui précède l'entête AH et les données

### ➤ ESP (encapsulating security payload)

ESP est le second protocole de protection des données qui fait partie de la spécification IPsec il ne protège pas les en-têtes des datagrammes IP utilisés pour transmettre la communication. Seules les données sont protégées. Il assure :

- **La confidentialité des données** : la partie donnée des datagrammes IP transmis est chiffrée
- **L'intégrité** : les données n'ont pas été modifiées depuis leur émission
- **L'authentification**: la partie donnée des datagrammes IP reçus ne peut avoir été émise que par l'hôte avec lequel a lieu l'échange IPsec
- **L'unicité**

### ❖ La gestion des clefs pour Ipsec:

**Ike**: a pour rôle la négociation, l'établissement, la modification et la suppression des associations de sécurité et de leurs attributs. Il pose les bases permettant de construire divers protocoles de gestion des clefs. Il comporte deux aspects principaux :

- phase 1, un ensemble d'attributs relatifs à la sécurité est négocié, les identités des entités sont authentifiées et des clés sont générées. Ces éléments constituent une première association de sécurité, dite SA ISAKMP.
- phase 2 permet de négocier les paramètres de sécurité relatifs à une association de sécurité à établir pour le compte d'un protocole de sécurité donné (par exemple AH ou ESP). Les échanges de cette phase sont protégés en confidentialité et intégrité/authentification grâce au SA ISAKMP.

**Ike** : utilise quatre modes : Le mode principal (Main mode), Le mode agressif (Aggressive Mode), Le mode rapide (Quick Mode), Le mode nouveau groupe (New Groupe Mode)

Main Mode et Aggressive Mode Les attributs suivants sont utilisés par Ike et négociés durant la phase 1 : un algorithme de chiffrement, une fonction de hachage, une méthode d'authentification et un groupe pour Diffie-Hellman, Trois clefs sont générées à l'issue de la phase 1 : une pour le chiffrement, une pour l'authentification et une pour la dérivation d'autres clefs, Quick Mode est un échange de phase 2. New Group Mode est un peu à part : Ce n'est ni un échange de phase 1, ni un échange de phase 2, mais il ne peut avoir lieu qu'une fois qu'une Isakmp est établie ; il sert à se mettre d'accord sur un nouveau groupe pour de futurs échanges Diffie-Hellman [10]

### ❖ Les deux modes de fonctionnement d'Ipsec :

**Le mode transport** : prend un flux de niveau transport (couche de niveau 4 du modèle OSI) et réalise les mécanismes de signature et de chiffrement puis transmet les données à la couche Ip. Dans Ce mode, l'insertion de la couche Ipsec est transparente entre Tcp et Ip. Tcp envoie ses données vers Ipsec comme il les enverrait vers IPv4.

L'inconvénient de Ce mode réside dans le fait que l'en-tête extérieur est produit par la couche Ip c'est-à-dire sans masquage d'adresse.

**Le mode tunnel** : les données envoyées par l'application traversent la pile de protocole jusqu'à la couche Ip incluse, puis sont envoyées vers le module Ipsec. L'encapsulation Ipsec en mode tunnel permet le masquage d'adresses. Le mode tunnel est utilisé entre deux passerelles de sécurité (routeur, firewall, ...) alors que le mode transport se situe entre deux hôtes.

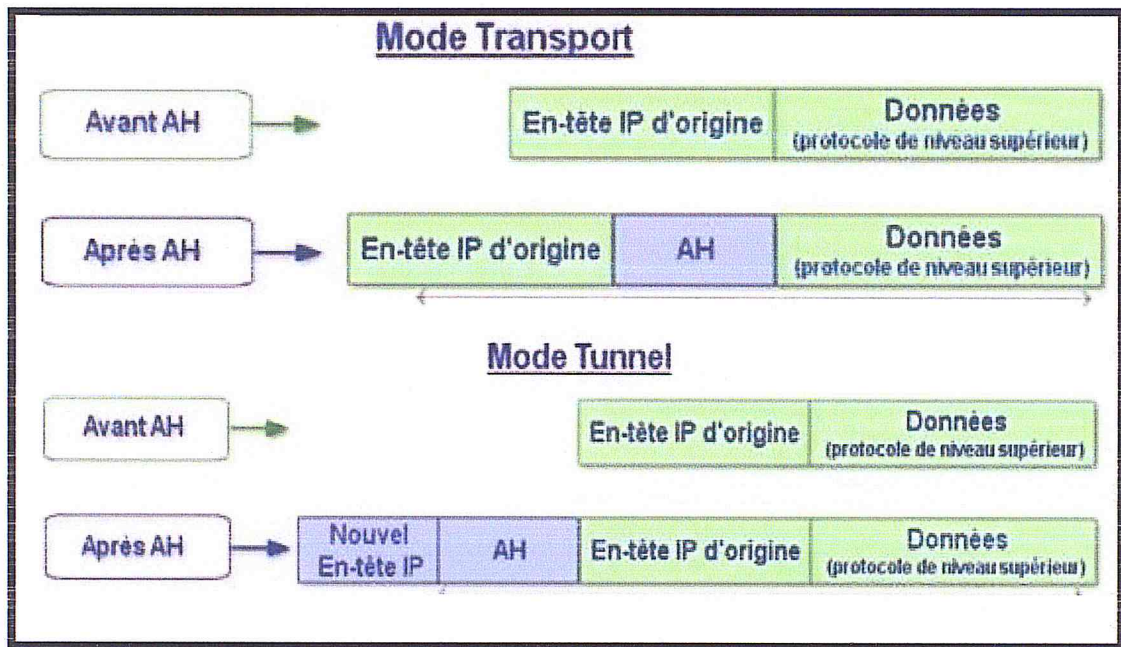


Figure I.08 : les deux modes de fonctionnement d'IPSec

## 5.2. Authentification

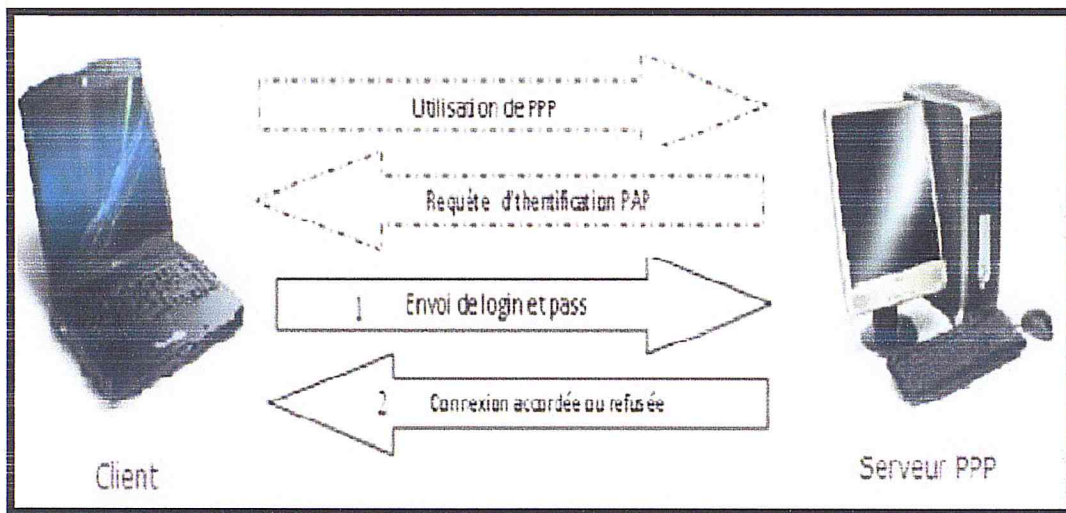
L'authentification est la procédure qui consiste, pour un système informatique, à vérifier l'identité d'une personne ou d'un ordinateur afin d'autoriser l'accès de cette entité à des ressources (systèmes, réseaux, applications...).

### 5.2.1 Les protocoles d'authentification

#### ❖ Le protocole PAP

Le protocole PAP (Password Authentication Protocol), utilisé avec le Protocole PPP, permet d'identifier un utilisateur auprès d'un serveur PPP en vue d'une ouverture de connexion sur le réseau. Après une phase de synchronisation entre le client et le serveur pour le définir l'utilisation du Protocole PPP et PAP, le processus d'authentification se fait en deux étapes :

- Le client envoie son nom PAP ainsi que son mot de passe en clair.
- Le serveur qui détient une table de noms d'utilisateurs et de mots de passe vérifie que le mot de passe correspond bien à l'utilisateur et valide ou rejette la connexion [11].



**Figure I.09 : Authentification du protocole PAP**

PAP est le plus simple des Protocoles d'authentification, il est donc très facile à implémenter. Mais étant donné que le mot de passe circule en clair sur le réseau, c'est aussi le moins sécurisé, il est donc fortement déconseillé. D'autre part, même si le mot de passe est crypté, il est toujours possible d'utiliser un sniffer afin de capturer la requête d'authentification et la réutiliser pour s'authentifier, c'est ce qu'on appelle : attaque par rejeu.

### Le Protocole CHAP

Contrairement au Protocole PAP, le Protocole CHAP (Challenge Handshake Authentication Protocole) permet une authentification sécurisée par hachage MD5 (Message Digest 5). MD5 est une fonction de hachage cryptographique permettant d'obtenir l'empreinte numérique d'un message à partir de laquelle il est impossible de retrouver le message original. Ainsi, en envoyant l'empreinte du mot de passe au serveur, le client peut montrer qu'il connaît bien le mot de passe sans avoir à réellement l'envoyer sur le réseau. Après le même type de synchronisation que pour le Protocole PAP, le mécanisme d'authentification est basé sur un CHALLENGE en 3 étapes : [12]

- Le serveur envoie au client un nombre aléatoire de 16bits ainsi qu'un compteur incrémenté à chaque envoi.
- Le client génère une empreinte MD5 de l'ensemble constitué reçu puis il envoie cette empreinte.

- Le serveur calcule également de son côté l’empreinte MD5 grâce au mot de passe du client stocké localement puis il compare son résultat à l’empreinte envoyée par le client. Si les deux empreintes sont identiques, le client est bien identifié et la connexion peut s’effectuer sinon, elle est rejetée.

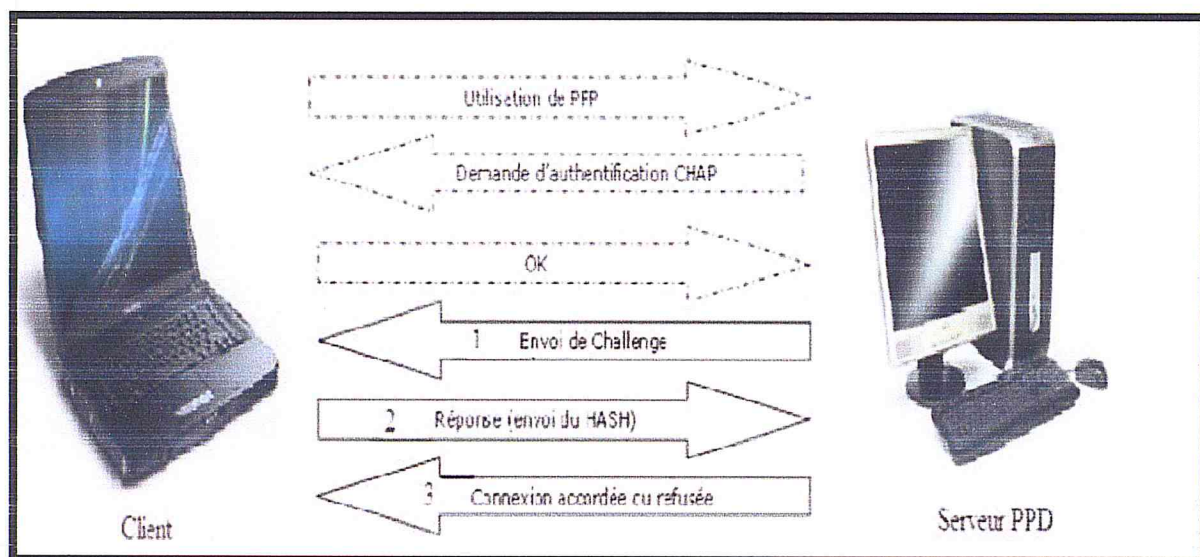


Figure I.10 : authentification du protocole CHAP

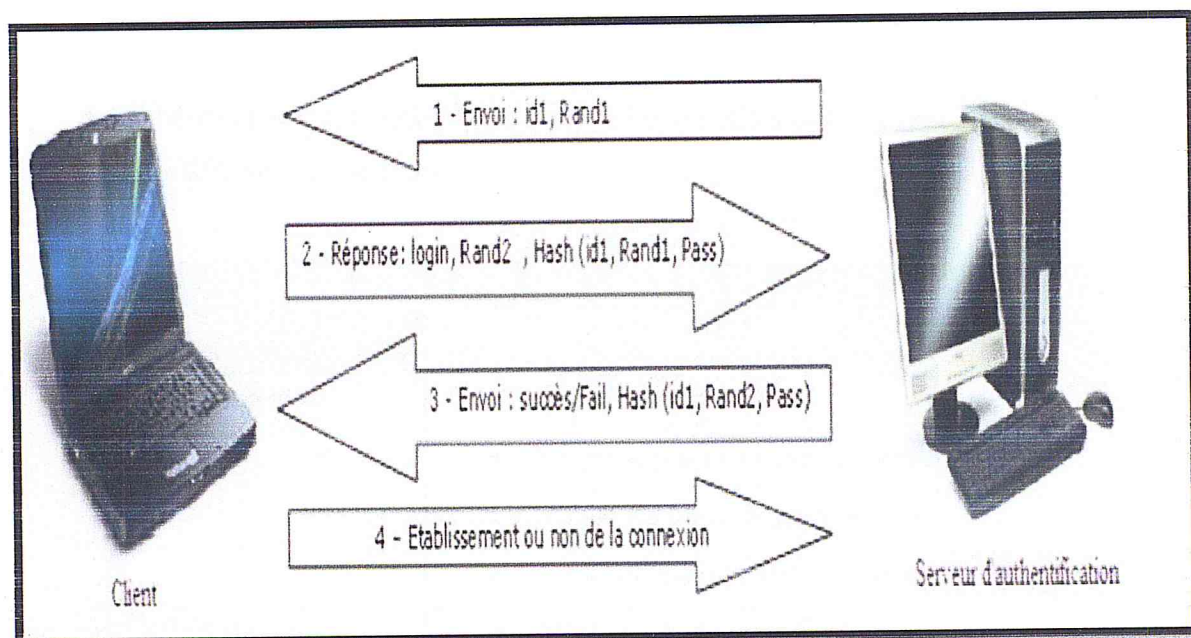
### ❖ Le protocole MS-CHAP

MS-CHAP (Microsoft Challenge Handshake Authentication Protocol) est la version spécifique de CHAP mise au point par Microsoft. Plus qu’une simple version prioritaire, MS-CHAP apporte également quelques améliorations à CHAP. Un des principaux inconvénients de CHAP est que le serveur doit détenir les mots de passe des utilisateurs en clair pour pouvoir vérifier l’empreinte MD5 envoyée par les clients, ce qui constitue une vulnérabilité potentielle en cas de compromission du serveur. Pour remédier à cette faiblesse, le Protocole MS-CHAP intègre une fonction de hachage propriétaire permettant de stocker sur le serveur un hash intermédiaire du mot de passe. Ainsi, en travaillant uniquement avec ce hash intermédiaire au lieu du mot de passe, le client et le serveur peuvent réaliser le même type de procédure que celle du CHAP, ainsi, le mot de passe en clair n’a plus besoin d’être stocké sur le serveur. Puis malgré l’avancée du Protocole MSCHAP par rapport à CHAP, Microsoft créa une seconde version du Protocole (MS-CHAP-v2) pour résoudre deux principales faiblesses de MS-CHAP-v1, d’une part le fait que le client ne puisse pas vérifier l’authenticité du serveur sur lequel il veut se connecter et d’autre part que l’algorithme de hachage propriétaire utilisé soit très vulnérable à des attaques par brute-force [13].

## Chapitre I : Généralité

Voici le fonctionnement du processus d'authentification mutuelle fournit par MS-CHAP-v2 :

- Le serveur d'accès disant envoie une demande de vérification au client contenant une identification de session I et une chaîne C1 générée aléatoirement.
- Le client envoie alors une réponse contenant : son nom d'utilisateur, une chaîne aléatoire C2 et un hash de l'ensemble formé par la chaîne C1, l'identificateur de session I et son mot de passe.
- Le serveur vérifie la réponse du client et il renvoie une réponse contenant : une chaîne indiquant le succès ou l'échec de l'authentification, et un hash de l'ensemble formé par 3 éléments : la chaîne C2, l'identificateur de session I et son mot de passe.
- Le client vérifie à son tour la réponse d'authentification et établit la connexion en cas de réussite.



**Figure I.11 : Authentification du protocole MS-CHAP**

Cette méthode d'authentification est bien mutuelle car elle permet effectivement au client d'être sûr de l'identité du serveur car seul le serveur peut lui renvoyer son mot de passe dans le hash à l'étape 3.

### ❖ Le protocole EAP (Extensible Authentication Protocol)

La méthode d'authentification EAP utilise différents éléments pour identifier un client

		<ul style="list-style-type: none"><li>• Authentification mutuelle</li></ul>
EAP-PEAP	-Login/password -Certificat	<ul style="list-style-type: none"><li>• Similaire à EAP-TTLS</li><li>• Création d'un tunnel TLS sûr</li><li>• Authentification mutuelle</li></ul>

Tableau I.2 : les types d'authentification en utilisant EAP

### 5.3. Pare-feu (Firewall)

Le Firewall est un système qui permet à une organisation de mettre en place un périmètre de sécurité entre Internet et son réseau informatique interne.

Il détermine :

- Les services internes pouvant accéder à l'extérieur (Internet).
- Les services externes pouvant accéder au réseau Interne

#### ❖ Listes de contrôle d'accès:

Une liste de contrôle d'accès est un ensemble séquentiel d'instructions d'autorisation ou de refus qui s'appliquent aux adresses ou au protocole de la couche supérieure. Les listes de contrôle d'accès représentent un outil puissant pour contrôler le trafic entrant ou sortant d'un réseau

#### ❖ Types de liste de contrôle d'accès:

Les deux grandes catégories des ACLs sont :

- **ACL standard** : Les ACLs standard permettent d'autoriser et de refuser le trafic en provenance d'adresse ip source, la destination du paquet et le port concernés non aucune incidence.
- **ACL étendu** : Les ACLs étendues filtrent les paquets ip en fonction de plusieurs attributs, L'adresse ip source, l'adresse ip destination, port source, port destination, protocole.

#### ❖ Positionnement des ACLs:

Chaque ACL doit être placée la ou elle aura le plus grand impact sur les performances. Les règles de base sont les suivants :



- login / mot de passe ;
- certificat électronique ;
- biométrie ; • puce (SIM).

Certaines méthodes combinent plusieurs critères (certificats et login/mot de passe etc.)

### ❖ Les différents types du protocole EAP

- **EAP-TLS** : authentification mutuelle entre le client et le serveur Radius par le biais de certificats (côté client et côté serveur).
- **EAP-TTLS et EAP-PEAP** : authentification mutuelle du client et du serveur Radius par le biais d'un certificat côté serveur, le client peut utiliser un couple login/mot de passe.
- **EAP-MD5** : pas d'authentification mutuelle entre client et le serveur Radius, le client s'authentifie par mot de passe. [14]

Type EAP	Méthode d'authentification	Remarque
EAP-MD5	Login/password	<ul style="list-style-type: none"><li>• Facile à implémenter</li><li>• Supporté par beaucoup de serveur</li><li>• Utilise les mots de passe en clair</li><li>• pas d'authentification mutuelle</li></ul>
EAP-TLS	Certificat	<ul style="list-style-type: none"><li>• Utilisation de certificats pour le serveur et les clients</li><li>• Solide mais plus compliqué à gérer à cause des certificats</li><li>• Authentification mutuelle entre le serveur et le client</li></ul>
EAP-TTLS	-Login/password -Certificat	<ul style="list-style-type: none"><li>• Création d'un tunnel TLS sûr</li><li>• Supporte PAP, CHAP, MS-CHAP, MS-CHAPv2</li><li>• Certificat obligatoire côté serveur, optionnel côté client</li></ul>

- Placez les ACLs étendues le plus près possible de la source du trafic
- Placez les ACLs standard le plus près possible de la destination.

❖ **ACL numéroté et ACL nommée**

- **ACL numéroté**

Au moment de configurer les listes de contrôle d'accès il faut identifier chaque liste de protocole en lui attribuant un numéro unique. Le numéro choisi pour identifier une liste de contrôle d'accès doit se trouver à l'intérieur d'une plage précise, valable pour le protocole:

Type d'ACL	Plage de numéros
ACL standard	1 à 99 et 1300 à 1999
ACL étendu	100 à 199 et 2000 à 2699

Tableau I.3: les plages des ACLs et leurs types

- **ACL nommée**

Les ACL nommées sont utilisées pour pouvoir donner un nom à notre ACL et ne plus les identifier par un numéro. En effet on pourra lui donner un nom explicite ce qui nous aidera à déterminer plus facilement le but de notre ACL.

❖ **Les ACLs Reflexives**

Les ACL réflexives permettent de prendre en compte les retours de connexions. Ces ACL sont définis en entrée ou en sortie. Le but est d'effectuer un suivi de la connexion en n'autorisant le trafic que dans un sens seulement s'il est précédé d'un trafic dans l'autre sens. [15].

❖ **Les ACLs dynamiques**

Les ACL dynamiques obligent l'utilisateur à établir une connexion Telnet sur le routeur en fournissant à ce dernier une combinaison nom d'utilisateur/ mot de passe, pour autoriser le trafic de cette utilisateur. Si l'authentification Telnet a réussi, le routeur modifie dynamiquement l'ACL associée, autorisant le trafic provenant de l'IP de l'utilisateur. [16]

❖ **Les ACLs Datés**

Elles autorisent un contrôle d'accès basé sur l'heure. Une plage temporelle est créée qui définit des heures spécifiques de la journée et de la semaine afin d'implémenter des listes de

contrôle d'accès basées sur l'heure. La plage temporelle est identifiée par un nom et référencée par une fonction.

### ❖ Les CBAC

Les CBAC de Cisco fournissent un nouveau mécanisme de filtrage basé sur l'état des connexions. Elles examinent non seulement les informations des couches réseau et transport mais examinent aussi les informations de la couche application (comme ftp) pour apprendre et inspecter l'état des sessions TCP et UDP. Les CBAC maintiennent des informations d'état des connexions, pour chaque connexion, dans leurs propres structures de données. Ces informations d'état sont utilisées pour prendre les décisions sur quels paquets doivent être autorisés ou refusés. A la fermeture d'une session, l'entrée des ACL associée est effacée.

- **Fonctionnement des CBAC**

Les paquets arrivant sont comparés à l'access-list de l'interface associée. Si le paquet est autorisé à transiter (ACL), il est inspecté. S'il initialise une nouvelle connexion ou ouvre un nouveau port de donnée, l'access-list correspondante est modifiée pour permettre aux paquets relatifs à la nouvelle connexion de passer. Les paquets sont inspectés quand ils entrent ou sortent d'un réseau protégé, pour chaque interface configurée pour l'inspection par les CBAC.

Une entrée de la table d'état est créée si le paquet est celui commençant une nouvelle session TCP ou s'il est le premier paquet UDP contenant une adresse et un port non récent. Le trafic de retour n'est permis que si la table d'état contient des informations indiquant que le paquet appartient à une session valide. Quand la session se termine (TCP) ou finit (Time-out) l'entrée de la table d'état d'une session est effacée. [17]

- **Les avantages des CABC**

- **bloquer les attaques DoS**

- **ip inspect tcp synwait-time seconds** : Spécifie combien le firewall laissera de temps pour que la connexion TCP atteigne l'état "établie"
- **ip inspect tcp finwait-time seconds** : Spécifie combien le firewall attendra de temps l'échange des bits FIN avant d'interdire la session

- **CBAC génère des alertes temps réel:** ip inspect alert-on

#### 5.4. IDS

Systemes de détection d'intrusions, sont des systèmes software ou hardware conçus afin de pouvoir automatiser le monitoring d'événements survenant dans un réseau ou sur une machine particulière, et de pouvoir signaler à l'administrateur système, toute trace d'activité anormale sur ce dernier ou sur la machine surveillée .L'IDS est un système de détection passif.[18]

##### ❖ Principes de détection:

Nous classons les IDS en deux grandes catégories de principe de détection d'intrusion :

- **Approche par scénario:** Les systèmes à base de signatures qui consistent à rechercher dans l'activité de l'élément surveillé les empreintes d'attaques répertoriées et donc connues
- **Approche comportementale:** Les systèmes à approche comportementale consistent à détecter les différentes anomalies sur le réseau. C'est l'administrateur qui définira le fonctionnement "normal" des éléments surveillés, il y a donc une phase d'apprentissage pour fixer ce niveau

##### ❖ Type d'IDS:

- **Network based IDS (NIDS):** analyser de manière passive les flux en transit sur le réseau et détecter les intrusions en temps réel.
- **Host Based IDS (HIDS):** surveille le trafic sur une seule machine. Il analyse les journaux systèmes, les appels systèmes et enfin vérifie l'intégrité des systèmes de fichiers

#### 5.5. IPS

Un système de prévention d'intrusion peut être n'importe quel outil qui utilise le contrôle d'accès pour protéger un système d'un abus de la part d'attaquant , conçu pour être installé en ligne par rapport au flux du trafic et prévenir les attaques en temps réel il a la capacité de vérifier les protocoles de la couche 7 comme :HTTP,FTP,SMTP permettant une meilleur prise

de conscience ,il peut corriger le CRC, flux de paquet défragmenté ,prévenir les problèmes de séquençages TCP et nettoyer les options indésirable de la couche transport et réseaux

Plusieurs stratégies de prévention d'intrusions existent :

**host-based memory and process protection:** surveille l'exécution des processus et les tue s'ils ont l'air dangereux (buffer overflow). Cette technologie est utilisée dans les KIPS (Kernel Intrusion Prévention System)

**Interception de session:** termine une session TCP avec la commande TCP Reset : «RST». Ceci est utilisé dans les NIPS (Network Intrusion Prevention System).

**Gateway intrusion détection:** si un système NIPS est placé en tant que routeur, il bloque le trafic ; sinon il envoie des messages à d'autres routeurs pour modifier leur liste d'accès.

❖ **Type d'IPS:**

1. **Host Based IPS (HIPS):**complémente les traditionnels méthodes d'antivirus heuristique et basé empreinte il réside sur une adresse ip spécifique sur un ordinateur unique
  2. **Network based IPS (NIPS):**Application ou matériel qui empêche toute intrusion sur un réseau spécifique, Les NIPS peuvent être basé contenu ou basé taux
- **IPS :** se rattache à l'intention de l'attaque plutôt qu'au contenu, prévient d'attaque Dos et DDos
  - **CIPS:** inspecte le contenu des paquets à la recherche de séquences unique (signature).

## 5.6. Honeypot

Une ressource d'un réseau qui accroît la sécurité en étant mis à l'épreuve, attaquée ou effectivement compromise. Ce leurre permet de récupérer des informations des méthodes, tactiques et outils des pirates, Un honeypot n'a aucune valeur de production, tout ce qui entre ou sort d'un honeypot est probablement un sondage ou une attaque [19]

❖ **Niveau d'interaction de honeypot:**

Les honeypots sont principalement divisés en deux catégories : les honeypots à faible interaction et les honeypots à forte interaction

- **Niveau interaction faible:** émule des faux services réseaux qui sont vulnérables, il les simule par l'intermédiaire de script. Avec ce type d'honey-pot, le pirate n'interagit jamais avec le système d'exploitation même s'il en a l'impression. La sécurité est donc ainsi conservée.
- **Niveau interaction fort:** ne sont pas basés sur l'émulation de services ou de systèmes d'exploitation. Au contraire, ils reposent sur un vrai système d'exploitation où de véritables services, vulnérables ou non, tournent et sont accessibles aux pirates. Ainsi, la méthode d'approche est complètement différente puisque l'on offre au pirate la possibilité de rentrer dans le système et de faire ce qu'il lui plaît une fois le système compromis.

### 5.7. Les serveurs proxy:

Un serveur proxy est un ordinateur qui sert d'intermédiaire entre un navigateur Web (tel qu'Internet Explorer) et Internet. Les serveurs proxy permettent d'optimiser les performances Web en stockant la copie des pages Web souvent utilisées. Lorsqu'un navigateur requiert une page Web qui est stockée par le serveur proxy (dans le cache de celui-ci), il est servi par ce dernier, et donc plus rapidement qu'en allant sur le Web. Les serveurs proxy renforcent également la sécurité en filtrant certains contenus Web et les logiciels malveillants. [20]

### 5.8. L'antivirus

La meilleure protection contre les infections reste l'antivirus, bien que le nombre de virus augmente chaque jour et que les antivirus ne soient pas capables de tous les détecter. Les antivirus doivent donc être mis à jour régulièrement afin de contenir le plus de définitions de virus possible, ce qui peut s'effectuer de manière automatique. La détection d'un virus s'effectue par la recherche de fragments de code malicieux, correspondant à sa signature. Il se pose ici le problème des virus polymorphes, capables de modifier leur signature durant leur réplique. C'est pour cela que les logiciels antivirus sont capables de détecter des comportements anormaux, mais cette détection difficile ne peut en aucun cas dispenser des mises à jours fréquentes. Deux techniques de protection sont offertes. La première est l'analyse automatique de tout fichier accédé de la machine. La seconde consiste à lancer une analyse complète du système. Cette analyse nécessitant beaucoup de ressources est donc réalisée ponctuellement.

### **Conclusion**

Les systèmes informatiques et plus précisément les systèmes d'information sont vitaux au bon fonctionnement de toute entreprise. Il est donc nécessaire d'assurer leurs protections, afin de lutter contre les menaces qui pèsent sur l'intégrité, la confidentialité et la disponibilité des ressources.

La malveillance informatique est souvent à l'origine de ces menaces, qu'il s'agisse de vol d'information ou de sabotage, n'importe qui pouvant s'improviser pirate informatique avec des outils adaptés.

Nous avons essayé dans ce premier chapitre de recenser toutes les menaces et attaques susceptibles de toucher à tout système tel que l'attaque HSRP et DHCP. Toute cette étude a été menée pour nous aider à entamer notre travail au sein de notre organisme d'accueil afin de déceler toutes les éventuels risques, menaces et attaques pouvant nuire à l'entreprise.

Dans le chapitre suivant nous allons essayer d'étudier le système informatique de notre organisme d'accueil à savoir « Saidal », de comprendre tous les risques liés à sa sécurité informatique, et finalement de proposer et de construire une politique de sécurité adaptée aux besoins de notre structure.

### **Introduction**

Dans nos jours l'entreprise demande beaucoup des compétences nécessaires pour garantir une sécurité optimale tel qu'elle minimise les risques des attaques. Mais est ce que possible de garantir la sécurité d'information à 100%., Malgré tout ce qu'il existe comme des moyens efficaces pour faire face à ces attaques.

C'est pour cela qu'il est utile de bien savoir gérer les ressources disponibles et comprendre les risques liés à la sécurité informatique, pour pouvoir construire une politique de sécurité adaptée aux besoins de la structure à protéger. La mise en place d'un dispositif de sécurité efficace ne doit cependant jamais dispenser d'une veille régulière au bon fonctionnement du système.

Ce chapitre sera consacré à la présentation de l'organisme d'accueil « le Groupe SAIDAL» ainsi que tous ses besoins en terme de la sécurisation de son système et son réseau informatiques.

Nous allons par la suite décrire les solutions proposées aux insuffisances du réseau actuel, elles comprendront une architecture et une nouvelle politique de sécurité qui devront être en conformité totale avec la politique de l'entreprise.

Pour cela, il sera question de faire des choix à savoir la technologie d'interconnexion entre les sites des protocoles implémentés pour véhiculer les données de l'entreprise de manière sûre et fiable, un mécanisme qui assure l'identité des utilisateurs internes de l'entreprise et une technologie qui permet aux utilisateurs d'accéder à Internet plus rapide.

Ce chapitre se compose de trois principales parties :

1. Passerelle internet
2. Datacenter
3. Authentification RADIUS

### **1. Présentation de l'organisme d'accueil**

Le groupe industriel SAIDAL est une société par action (SPA) au capital social de 2500, 000,000 dinars algériens dont la mission principale est de développer, produire et commercialiser pharmaceutique à usage humain et vétérinaire, le groupe SAIDAL est considéré actuellement comme le leader de l'industrie pharmaceutique en Algérie avec une grand part de marche



# Chapitre II

## Développement de notre politique de sécurité

## **1.2 Historique**

SAIDAL a été créée en avril 1982 à la suite de la restructuration de la pharmacie centrale algérienne (PCA) et à bénéficier, dans ce cadre, du transfert de usines d'EL Harrach, de Dar El-Beida et Gué de Constantine, il a été également transfère en 1988, le complexe 'Antibiotique' de Médéa dont la réalisation venait d'être achevé par la SNIC (Société National de Industries Chimiques).

En 1989 et suite à la mise en œuvre des référence économique SAIDAL devient une entreprise publique économique dotée de l'autonomie gestion

En 1993, des changements ont été apportés aux statuts de l'entreprise, lui permettant de participer à toute opération industrielle ou commerciale pavant se rattacher à l'objet social par voie de création de société nouvelle ou de filiales

En 1997, la société SAIDAL à mise en œuvre un plan de restructuration qui s'est traduit par sa transformation en groupe industriel regroupant trois filiales (Pharmal, Antibiotical et Biotic).

En 2009, SAIDAL a augmenté sa part dans le capital SOMEDIAL à hauteur de 59%. En 2010, elle a acquis 20% du capital d'IBERAL et sa part dans le capital de TAPHCO est passée de 38 ,75% à 44,51%

En 2011, SAIDAL a augmenté sa part dans le capital d'IBERAL à hauteur de 60%.

En janvier 2014, SAIDAL a procédé par voie d'absorption, à la fusion de ses filiales détenues à 100% : Pharmal, Antibiotical et biotic. [webc]

## **1.3. Les Missions**

En tant que premier producteur de médicaments génériques en Algérie, la mission première de SAIDAL c'est :

- De contribuer à la protection de la santé des citoyens et à l'amélioration de la qualité des soins par la mise à disposition des patients, d'une gamme riche et diversifiée de produit de qualité
- De protéger le droit des citoyens d'accéder aux traitements par l'adaptation d'une politique tarifaire favorisant de larges couches de la société

Sa position d'entreprise publique lui confier également la mission d'accompagner la politique de santé publique dans le développement de l'industrie pharmaceutique par le choix d'investissement orientés vers la satisfaction des besoins de la population. [Webc]

#### **1.4. Organigramme générale du Groupe SAIDAL**

Le Groupe SAIDAL a procédé en janvier 2014 à la fusion, par voie d'absorption, des filiales Antibiotical, Pharmal et Biotic. Cette décision approuvée par ses organes sociaux a donné lieu à une nouvelle organisation s'articulant autour de :

- Une direction générale
- Neuf (09) sites de production
- Trois centres de distribution

Cette structure organisationnelle est détaillée par l'organigramme suivant :

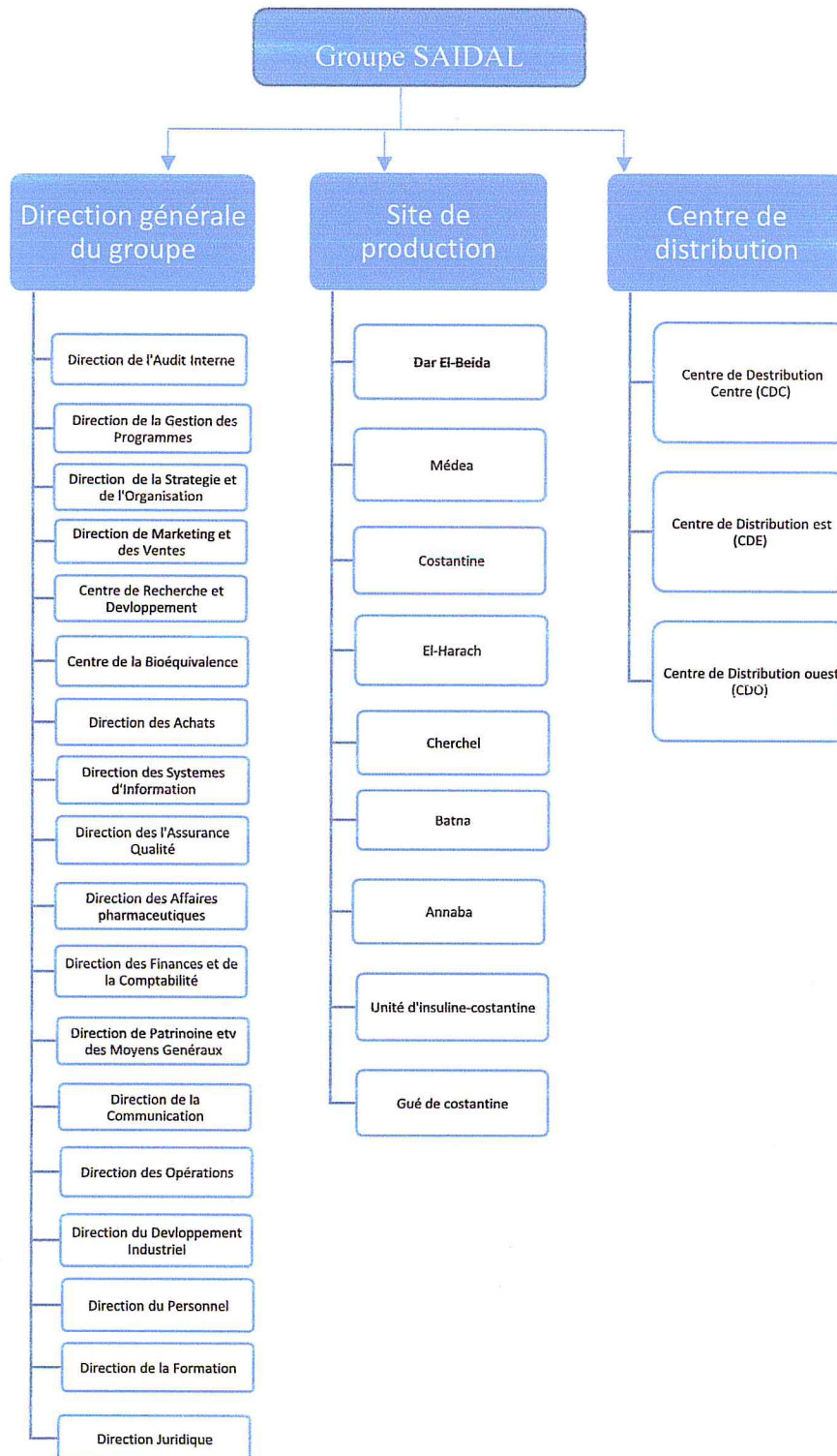


Figure II.01 : Organigramme générale du Groupe SAIDAL

### **1.5. Site de production de Dar El-Beida**

C'est le site dans lequel nous effectuons notre stage, il existe depuis 1958, il appartenait au laboratoire français LABAZ avant nationalisation en 1970, ce qui donné lieu aux transformations suivant :

- Agrandissement du site de 3600 m<sup>2</sup> à 6600 m<sup>2</sup>
- La mise au point des produits pharmaceutique algériens.
- Extension du magasin de stockage.
- Modernisation de chaines et ateliers

L'activité de site était limitée à la fabrication de quelques médicaments cométiques, mais actuellement elle produit une gamme de médicaments très large dans plusieurs forme génériques (comprimés, gélules, sirops, forme pâteuses, suspension buvable, sels et solution dermique).

Le site de production de Dar El-Beida est caractérisé par une capacité de production très importante (43 millions unités de vent par an), Aussi l'usine est dotée d'un laboratoire de contrôle de la qualité chargé de l'analyse physico-chimique et microbiologique et d'une surface de stockage de 6600 m<sup>2</sup> (4600 palettes [webc])

### **1.6. Lieu d'affectation du stage : la sous-direction de maintenance**

Notre étaie s'effectue au sein de la sous-direction de maintenance, qui est rattaché hiérarchiquement à la direction de l'usine, chargé du suivi de l'entretien des équipements et des ateliers de production, l'organigramme suivant présente la structure organisationnelle de la sous-direction de maintenance :

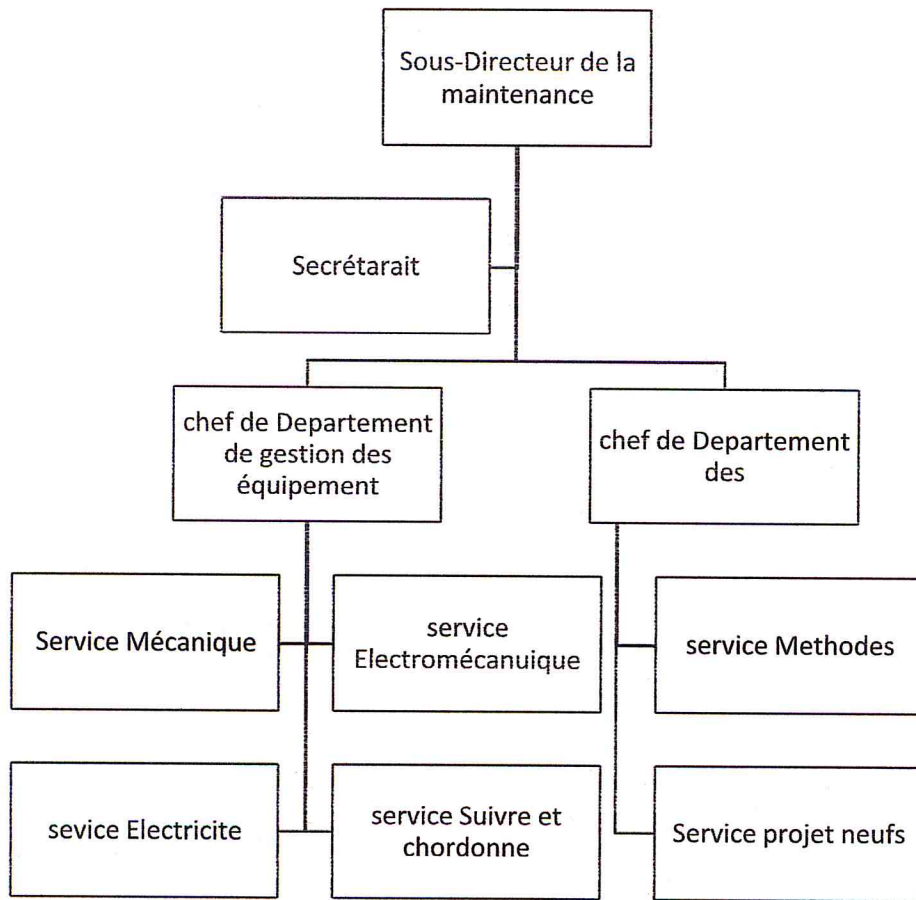


Figure II.02 : Organigramme de service de la maintenance

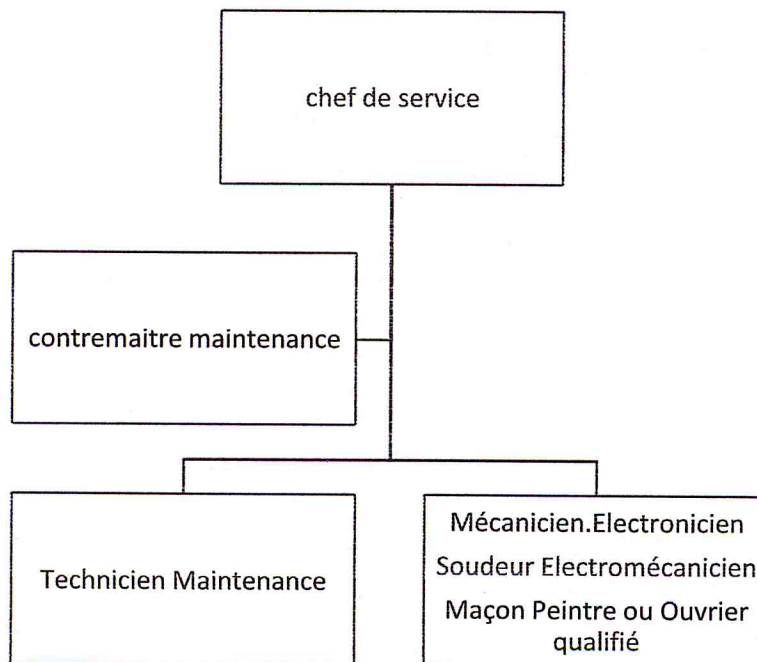


Figure II.03 : Décomposition d'un service

## 2. Présentation du sujet

Après plusieurs séances de travail effectuées avec les responsables de la cellule informatique au sein du groupe SAIDAL, nous avons pu extraire un ensemble d'insuffisances et de faille au sein de leur réseau informatique, à savoir les 3 grands problèmes :

- Problème de Sécurité lors d'accès internet (authentification + contenu)
- Problème de sécurité lors de l'interconnexion site-to-site (extranet)
- Problème d'accès et de disponibilité des données locales en toute sécurité

## 3. Plan général du réseau informatique de Groupe SAIDAL

La topologie ci-dessous illustre l'architecture générale du réseau de Groupe SAIDAL:

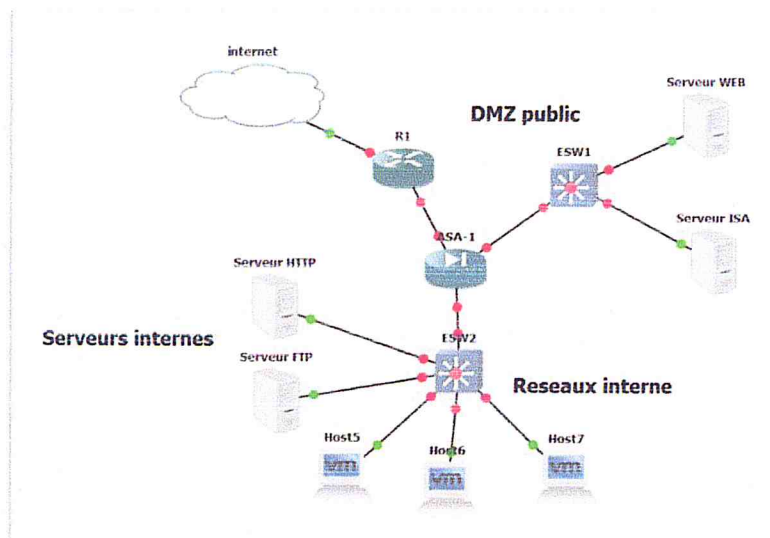


Figure II.04: plan initial de réseau de Groupe SAIDAL

Pour cela, notre objectif principal est de proposer une politique de sécurité basée sur (les protocoles utilisés) et qui devra être en conformité totale avec la politique de l'entreprise.

## 4. Notre solution :

Il sera question de faire des choix à savoir la technologie d'interconnexion entre les sites des protocoles implémentés pour véhiculer les données de l'entreprise de manière sûre et fiable, un mécanisme qui assure l'identité des utilisateurs interne de l'entreprise et une technologie qui permet aux utilisateurs d'accéder à Internet plus rapide.

Cette solution se composera de trois principales parties à savoir :

1. Partie Passerelle internet
2. Partie Datacenter
3. Partie Authentification RADIUS

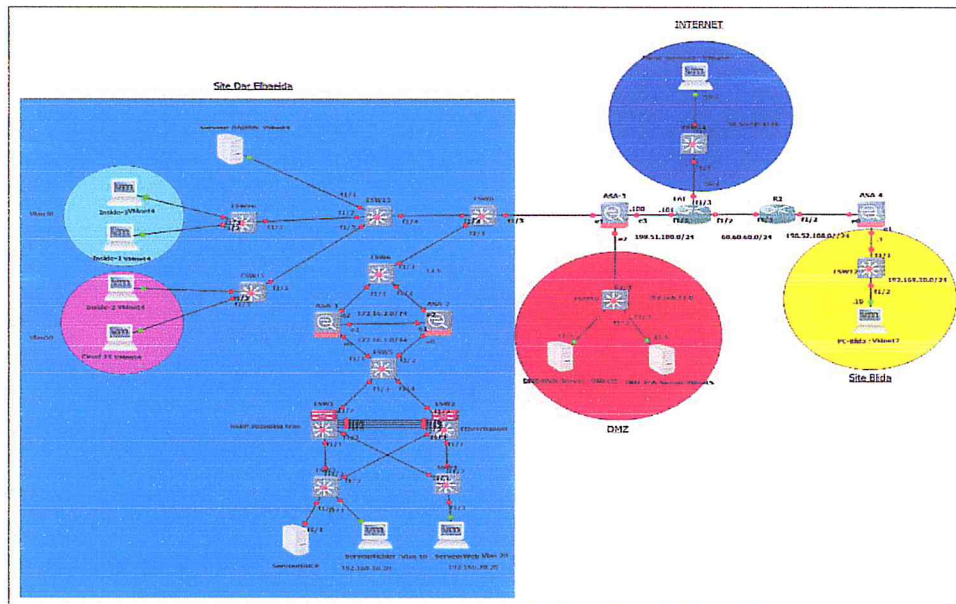
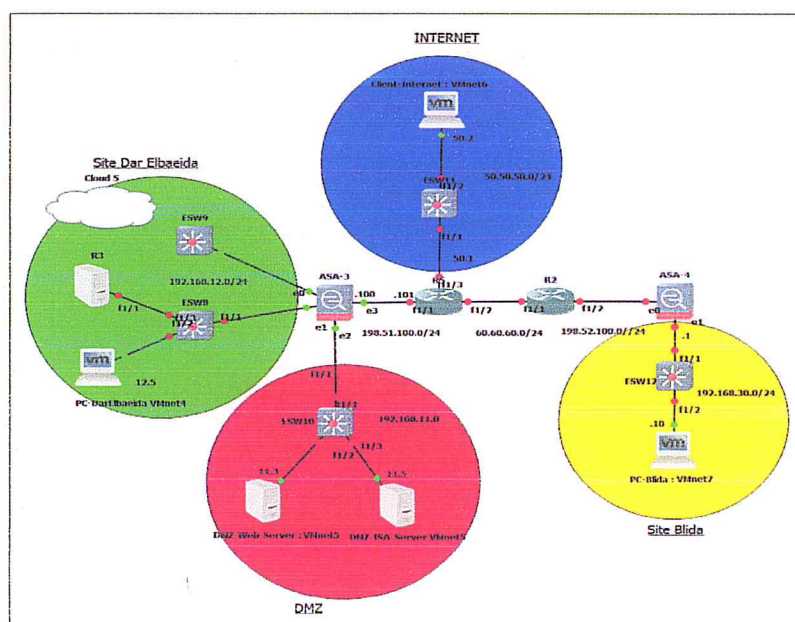


Figure II.05: plan général de réseau de Groupe SAIDAL

#### 4.1 Partie passerelle internet

Cette partie représente la passerelle internet du réseau de Groupe SAIDAL





### Figure II.06 : Architecture de la solution proposée (partie passerelle Internet)

Les utilisateurs de l'entreprise se trouvent dans la zone interne, et Internet est considéré comme une zone externe (zone non approuvée), La zone démilitarisée (DMZ) configurée pour services d'accès Internet tel que le serveur web, se situe entre la zone interne et externe (zone non approuvée) , mais lors de la réalisation de notre passerelle nous avons rencontré plusieurs problèmes parmi c'est dernier en a un problème major qui est le problème de sécurité lors de l'interconnexion site-to-site (extranet) , pour résoudre ce dernier nous avons opté a une politique de sécurité suivante :

- Traduire les adresses de réseau interne à l'aide du NAT
- Permettre au réseau interne l'accès à Internet à l'aide de proxy ISA serveur.
- Permettre au réseau interne l'accès aux réseaux DMZ
- Permettre l'accès Internet au réseau DMZ a l'aide du NAT statique
- Filtrage URL pour bloquer des sites web (blacklist)
- Serveur de mise en cache pour réduire le temps d'accès à Internet
- Seul le trafic autorisé transite sur le réseau de l'entreprise (intranet).
- Bloquer tout autre trafic
- vpn ipsec site to site entre site de Groupe SAIDAL et site Blida
- vpn remote access qui permet à l'administrateur d'accéder à l'entreprise depuis Internet

#### 4.1.1. Développement de la structure de l'inter-réseau

Les réseaux locaux d'entreprise (LAN) sont des réseaux internes à une organisation, c'est-à-dire que les liaisons entre machines appartiennent à l'organisation. Ces réseaux sont de plus en plus souvent reliés à internet par l'intermédiaire d'équipement d'interconnexion.il arrive ainsi que des entreprises éprouvent le besoin de communiquer avec des filiales ,des client ou même des personnels géographiquement éloigner via internet .pour autant, les données transmises sur internet sont beaucoup plus vulnérables que lorsqu'elles circulent sur un réseau interne à une organisation car le chemin emprunté n'est pas défini à l'avance ,ce qui signifie que les données empruntent une infrastructure réseau publique appartenant à différents opérateurs. Ainsi il n'est pas impossible que sur le chemin parcouru, le réseau soit écouté par un utilisateur indiscret ou même détourné. Il n'est donc pas concevable de transmettre dans telles conditions des informations sensibles pour l'entreprise

### 4.1.1.1. VPN site to site

La solution pour répondre au besoin de communication sécurisé consiste à relier chaque site de Groupe SAIDAL à internet avec une liaison spécialisée. Le Transfer des données entre les deux sites avec ligne spécialisés est en clair, sans cryptage ; donc il y a un risque de piratage des données pendant le transfert entre les deux sites. Ceci nous a ramené à opter pour le concept des réseaux virtuels privés (vpn) c'est à dire encapsulation les données à transmettre de façon chiffrées (VPN, acronyme de Virtual private network) .Le système de VPN permet donc d'obtenir une liaison sécurisées.

#### ❖ **Motifs de choix de la solution :**

- Les VPN créé un tunnel sécurisé entre deux ou plusieurs usagers sur n'importe quel réseau et s'appuient sur des technologies de chiffrement robuste et la mise en place des clés de chiffrement .Le niveau de confidentialité est donc très élevé.

#### ❖ **Choix du protocole au niveau de la couche réseaux:**

Aujourd'hui, le protocole le plus utilisé pour la mise en place des VPN est IPSEC (internet Protocole Sécurité) qui est un protocole de la couche 3 du modèle OSI .il est l'un des standard les plus diffusés, et les plus ouverts. IPSec offre plusieurs services : le chiffrement, le contrôle d'intégrité, l'authentification et le renouvellement périodique des clés. De plus, il est nativement implémenté dans IPv6 qui le rend par conséquent comme le protocole incontournable pour la communication sécurisés.

#### ❖ **Motifs de choix de la solution IPSEC:**

La stratégie IPSec permettant d'assurer la confidentialité, l'intégrité et l'authentification des données entre deux hôte est gérée par un ensemble de normes et de protocoles il a pour vocation de garantir:

- **Confidentialité :** IPSec crypte les paquets avant de les transmettre sur un réseau.
- **Intégrité :** les données n'ont pas été modifiées depuis leur émission

**L'authentification:** les paquets reçus ne peut avoir été émise que par l'hôte avec lequel a lieu l'échange IPsec.

**Protection anti-réémission:** IPSec empêche la capture et la réémission des paquets et contribue ainsi à déjouer les attaques par saturation.

❖ **Choix de l'Algorithme de chiffrement et fonction de hachage utilisé par le Protocol IPSEC :**

- S'agissant de l'algorithme de chiffrement utilisé par IPSec nous avons choisi l'algorithme 3des car il est suffisamment robuste pour chiffrer les données, de plus, il est facile à implémenter.
- Nous avons opté pour la SHA comme fonction de hachage afin de vérifier l'intégrité de nos données car il est le plus utilisé et simple à implémenter.

**4.1.1.2. VPN d'accès distant**

Cette solution est utilisée pour permettre à des utilisateurs itinérants d'accéder au réseau d'entreprise. L'utilisateur se sert d'une connexion Internet pour établir la connexion Vpn.

L'utilisateur possède son propre logiciel client pour le VPN auquel cas il établit directement la communication de manière cryptée vers le réseau de l'entreprise

**4.1.1.3. NAT**

Le mécanisme de translation d'adresses a été mis au point afin de répondre à la pénurie d'adresses IP avec le protocole IPv4 (le protocole IPv6 répondra à terme à ce problème).

En effet, en adressage IPv4 le nombre d'adresses IP routables (donc uniques sur la planète) n'est pas suffisant pour permettre à toutes les machines nécessitant d'être connectées à internet de l'être.

Le principe du NAT consiste à utiliser une adresse IP routable (ou un nombre limité d'adresses IP) pour connecter l'ensemble des machines du réseau en réalisant, au niveau de la passerelle de connexion à internet, une translation entre l'adresse interne (non routable) de la machine souhaitant se connecter et l'adresse IP de la passerelle.

**4.1.1.4. NAT statique**

Le Nat statique consiste à associer une adresse IP publique à une adresse IP privée interne au réseau (serveur web)

**4.1.1.5. ISA SEVER**

Cette solution offre plusieurs avantages pour l'entreprise qui souhaitent bénéficier d'une connectivité à Internet rapide et sécurisée [21]:

**1) Accès rapide au Web grâce à un cache très performant:**

ISA Server présente les avantages suivants en matière de performances Web :

- Il fournit aux utilisateurs un accès Web plus rapide en récupérant en local les objets non expirés plutôt que par le biais d'une connexion Internet plus lente et susceptible d'être encombrée
- Il réduit les coûts liés à la bande passante en diminuant le trafic réseau en provenance d'Internet.
- Il répartit le contenu de serveurs Web entre plusieurs serveurs pour un rendement optimal

**2) Connectivité à Internet sécurisée à l'aide d'un pare-feu multicouche**

ISA Server fournit les avantages suivants en termes de sécurité :

- Il protège les réseaux des accès non autorisés en inspectant le trafic réseau au niveau de plusieurs couches dans le modèle OSI
- Il protège le Web, le courrier électronique et d'autres serveurs d'applications d'attaques externes en utilisant la publication Web et la publication sur serveur pour traiter en toute sécurité les demandes entrantes adressées aux serveurs internes
- Il filtre le trafic réseau entrant et sortant pour garantir la sécurité
- Il active l'accès sécurisé pour les utilisateurs autorisés à partir d'Internet jusqu'au réseau interne en s'intégrant au service Routage et accès distant sur Windows Server pour implémenter des réseaux privés virtuels (VPN, Virtual Private Network) de manière sécurisée.

**3) Gestion unifiée avec administration intégrée:**

ISA Server fournit les avantages suivants en termes de gestion :

- Il contrôle l'accès de façon centralisée pour garantir et appliquer les stratégies d'entreprise
- Il améliore la productivité en limitant l'utilisation d'Internet aux applications, membres du personnel et destinations approuvés
- Il alloue la bande passante disponible en fonction des priorités de l'entreprise
- Il fournit des outils de surveillance et crée des rapports qui montrent comment la connectivité à Internet est utilisée
- Il automatise les tâches couramment effectuées à l'aide de script

### 4.1.1.5.1. Modes d'ISA Server:

Pour satisfaire les besoins de l'entreprise et des services en matière de sécurité et de performances, on peut installer ISA Server sous trois modes différents : le mode cache, le mode pare-feu et le mode intégré [22]

- **Mode cache:**

En mode cache, on peut améliorer les performances réseau et économiser de la bande passante en stockant les objets Web fréquemment utilisés sur l'ordinateur ISA Server le plus proche de l'utilisateur. On peut alors diriger les requêtes des clients vers un ordinateur ISA Server qui contient les objets mis en cache.

- **Mode pare-feu**

En mode pare-feu, on peut sécuriser le trafic réseau en configurant des règles qui contrôlent les communications entre un réseau interne et Internet. On peut également publier des serveurs internes qui permettent à une organisation de partager des données sur son réseau avec des partenaires ou des clients.

- **Mode intégré :** En mode intégré, nous pourrions combiner les services de pare-feu et de cache sur un seul ordinateur hôte. Bien que les organisations peuvent déployer ISA Server en tant que pare-feu séparé ou serveur de mise en cache séparé.

- ❖ **Choix du mode d'ISA serveur**

Nous allons utiliser pour notre implémentation le Mode intégré.

Cette partie permet aux utilisateurs de l'entreprise d'accéder au Datacenter en assurant la disponibilité des services (HTTP, HTTPS, FTP, DHCP).

### 4.2. Partie Datacenter

Cette partie permet aux utilisateurs de l'entreprise d'accéder au Datacenter en assurant la disponibilité des services (HTTP, HTTPS, FTP, DHCP).

### 4.2.1.L'architecture proposée

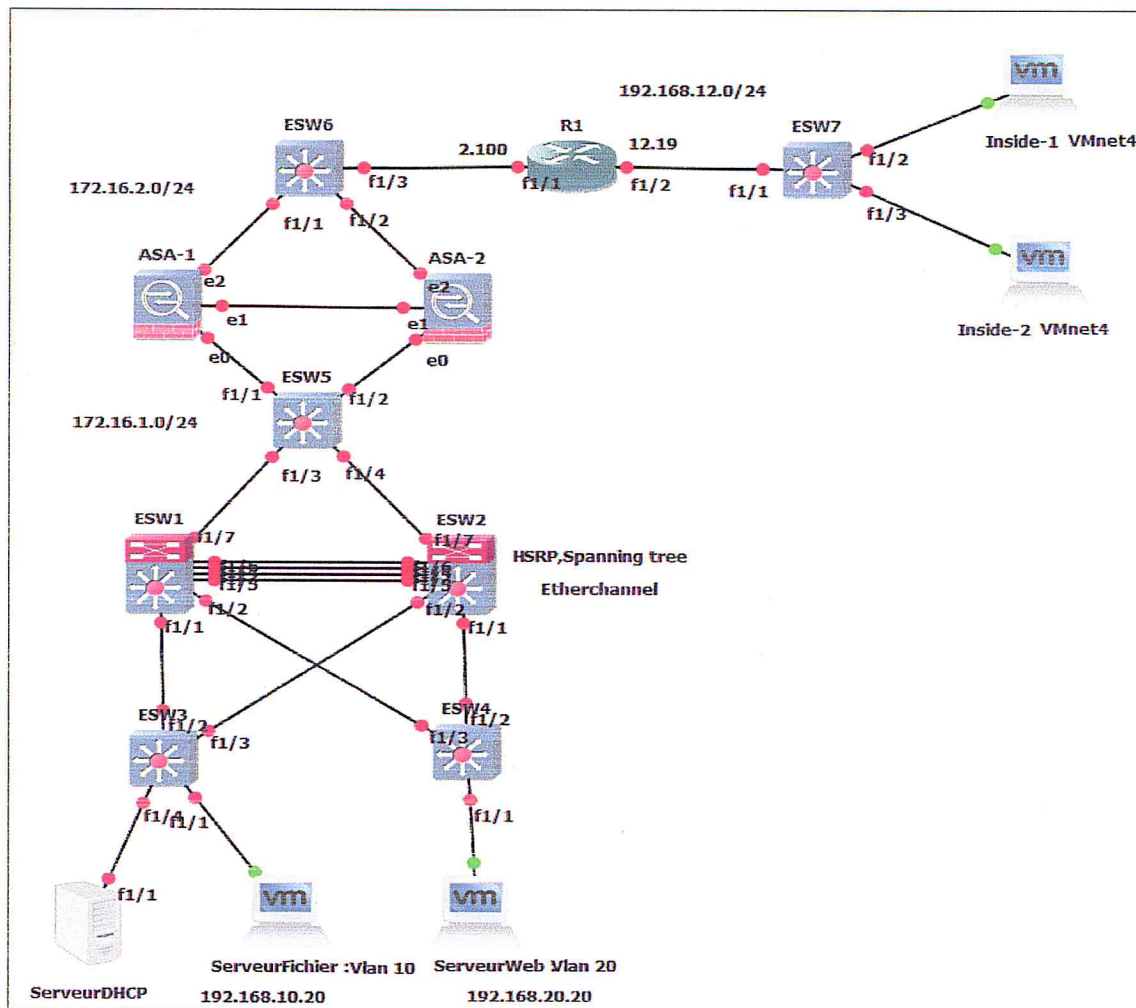


Figure II.07: Architecture de la solution proposée (partie Data Center)

### 4.2.2. La Redondance

#### 4.2.2.1. La Redondance des pare-feux

Au sein d'une infrastructure réseau, le firewall représente généralement un point de fêlure important, Nous allons donc mettre en place deux pare-feux afin de rendre l'architecture hautement disponible.

Notre choix porté sur le protocole FAILOVER car c'est le seul protocole qui assure la redondance pour La gamme ASA 8.4.2 .Celle-ci fonctionne en mode actif/passif, le second firewall ne prend la main que lorsque le premier connait une défaillance.

ASA utilise une interface HA (haute disponibilité) sur chaque firewall pour la réplique des modifications et le changement d'état entre les deux pare-feux.

### 4.2.2.2. Redondance des commutateurs

Nous allons utiliser le mécanisme de la redondance au niveau des Switch cores qui va nous permettre d'avoir des adresses ip virtuelle entre les deux Switch. Ainsi, si un commutateur est en panne, en maintenance ou bien est inaccessible, les équipements qui sont situés derrière ou avant ces commutateur continuent d'être joignables sans reconfiguration nécessaire

Notre choix du type de redondance de commutateur s'est porté sur les protocoles **HSRP** et **GLBP** et **Etherchannel**, **HSRP** et **GLBP** permet au ESW1 de gérer le trafic de vlan 10 et pour le ESW2 de gérer le vlan 20, en cas de panne ou de maintenance sur l'un des switches le trafic sera redirigé vers le deuxième Switch, **Etherchannel** permet d'assembler plusieurs liens physiques Ethernet en un lien logique. Le but est d'augmenter la vitesse et la tolérance aux pannes entre les deux Switch core

Nous allons utiliser le protocole **Spanning Tree** au niveau des Switch cores qui va nous permettre d'éviter les boucles dans le réseau.

### 4.2.3. Sécurité Datacenter

#### 4.2.3.1. Port Security

Cette option permet de définir une seule adresse MAC par ports et si cette adresse change le port se verrouille automatiquement. Cela permet de limiter la plupart des attaques ARP.

#### 4.2.3.2. Cache ARP statique

Ajouter des entrées statiques. Ainsi les passerelles par défaut et les serveurs important sont renseignés de manière définitive dans le cache ARP. De telles entrées n'expirent jamais et ne peuvent être mises à jour.

#### 4.2.3.3. DHCP Snooping

Le DHCP Snooping est un ensemble de techniques, agissant au niveau 2 du modèle OSI, La principe consiste à introduire la notion de confiance au niveau des interfaces des commutateurs. L'équipement sera configuré pour autoriser les DHCP Offer et DHCP Ack uniquement depuis les interfaces de confiance (trusted), les requêtes d'un poste utilisateur

tendant de se faire passer pour un serveur DHCP ne proviendront pas de l'interface de confiance seront donc supprimées.

### **4.2.3.4. Dynamic ARP Inspection (DAI)**

Cette fonction permet au commutateur de contrôler l'ensemble des requêtes ARP (ARP query, reply, Gratuitious ARP) afin de vérifier leur légitimité. Pour cela, il doit au préalable avoir connaissance de toutes les correspondances MAC / IP des postes directement connectés. A l'aide de la fonction DHCP Snooping présentée précédemment. Cette fonction analysant les requêtes DHCP garde une trace de toutes les affectations par DHCP des adresses IP et constitue une table MAC / IP réutilisée par DAI.

### **4.2.3.5 Listes de contrôle d'accès**

#### **4.2.3.5.1. Définition**

Une liste de contrôle d'accès est un ensemble séquentiel d'instructions d'autorisation ou de refus qui s'appliquent aux adresses ou au protocole de la couche supérieure. Les listes de contrôle d'accès représentent un outil puissant pour contrôler le trafic entrant ou sortant d'un réseau.

#### **4.2.3.5.2. Le filtrage des paquets**

Une liste de contrôle d'accès peut extraire les informations de l'en-tête des paquets, les valider conformément aux règles, et prendre des décisions d'autorisation ou de refus en fonction des critères suivants :

- Adresse IP source.
- Adresse IP destination.
- port source.
- port destination.
- Protocole.

Une liste de contrôle d'accès est un script de configuration de routeur contrôlant l'autorisation ou le refus de passage des paquets, conformément aux critères stipulés dans leur en-tête. Les ACL sont les objets les plus couramment utilisés dans le logiciel Cisco IOS.

À chaque fois qu'un paquet traverse une interface avec une liste de contrôle d'accès associé, celle-ci est vérifiée de haut en bas, ligne par ligne, à la recherche d'un modèle



correspondant au paquet entrant. L'ACL exécute au moins une stratégie de sécurité de l'entreprise en appliquant une règle d'autorisation ou de refus au paquet. On peut configurer des ACL en vue de contrôler l'accès à un réseau ou à un sous-réseau.

### 4.2.3.5.3 Règle des trois P

1. **Une ACL par protocole:** pour contrôler le flux du trafic sur une interface, il faut une ACL pour chaque protocole activé sur l'interface.
2. **Une ACL par direction:** les ACL contrôlent le trafic dans une seule direction à la fois sur une interface .il faut créer deux ACL: la première pour contrôler le trafic entrant et la seconde pour contrôler le trafic sortant.
3. **Une ACL par interface:** Les listes de contrôle d'accès contrôlent le trafic pour une interface. [23]

### 4.2.3.5.4. Fonctionnement des listes de contrôle d'accès

Les ACLs effectuent les taches suivantes :

- elles limitent le trafic réseau pour accroitre les performances réseau.
- elles contrôlent le flux de trafic .Les listes de contrôle d'accès peuvent limiter l'arrivée des mises à jour de routage.
- Elles fournissent un niveau de sécurité de base pour l'accès réseau .les ACLs permettent à un hôte d'accéder à une section du réseau tout en empêchant un autre hôte d'y avoir accès
- elle détermine le type de trafic à acheminer ou bloquer sur les interfaces de routeur

Les Acls définissent des règles de contrôle pour les paquets arrivant par les interfaces d'entrée, passant par le routeur et atteignant leur destination par les interfaces de sortie .Elles ne génèrent pas les paquets provenant du routeur lui-même.

- **ACL entrantes :** les paquets entrants sont traités avant d'être routé vers l'interface de sortie. Une liste d'accès entrante est efficace car elle réduit la charge des recherches de routage en cas d'abandon du paquet .si le paquet est autorisé à l'issue de tests, il est soumis au routage.
- **ACL sortante :** les paquets entrants sont routés vers l'interface de sortie puis traités par le biais de la liste de contrôle d'accès sortante.

### **4.3 Partie Authentification RADIUS**

#### **4.3.1. Authentification**

L'Authentification est la vérification d'informations relatives à une personne ou à un processus informatique. L'authentification complète le processus d'identification dans le sens où l'authentification permet de prouver une identité déclarée. Dans un serveur, un processus de contrôle valide l'identité et après authentification, donne l'accès aux données, applications, bases de données, fichiers ou sites Internet. Dans le cas contraire, l'accès est refusé.

#### **4.3.2. Radius**

RADIUS (Remote Authentication Dial-In User Service) est un protocole client-serveur permettant de centraliser des données d'authentification. Le protocole RADIUS a été inventé et développé en 1991 par la société Livingston, il a fait ultérieurement l'objet d'une normalisation par l'IETF, qui sera développé plus loin dans ce rapport.

#### **4.3.3 Fonctionnement de RADIUS**

Le fonctionnement de RADIUS est basé sur un scénario proche de celui-ci :

1. Un utilisateur envoie une requête au NAS afin de demander une connexion;
2. Le NAS achemine la demande au serveur RADIUS ;
3. Le serveur RADIUS consulte la base de données d'identification afin de connaître le type de scénario d'identification demandé pour l'utilisateur. Soit le scénario actuel convient, soit une autre méthode d'identification est demandée à l'utilisateur.

Le serveur RADIUS retourne ainsi une des quatre réponses suivantes :

- Access-Request : La conversation commence toujours par un paquet Access-Request émis par le NAS vers le serveur. Il contient au moins l'attribut User-Name et une liste d'autres attributs tels que Calling-Station-Id, Nas-Identifiant, etc.
- Access-Accept : ce paquet est renvoyé au NAS par le serveur RADIUS si l'authentification transmise par l'Access-Request a été correctement validée. Ce paquet contient alors des attributs qui spécifient au NAS les autorisations accordées par le serveur.
- Access-Reject : envoyé par le serveur RADIUS au NAS si l'authentification a échoué.

- Access-Challenge : après réception d'un paquet Access-Request, le serveur peut renvoyer un paquet Access-Challenge qui a pour but de demander d'autres informations et de provoquer l'émission d'un nouveau paquet Access-Request par le NAS.

Les paquets RADIUS utilisent les ports par défaut UDP 1812 pour authentification et l'autorisation et 1813 pour la Comptabilisation. Les ports 1645 et 1646 sont maintenant obsolètes.

Le diagramme ci-dessous présente l'usage des différents messages du protocole RADIUS.

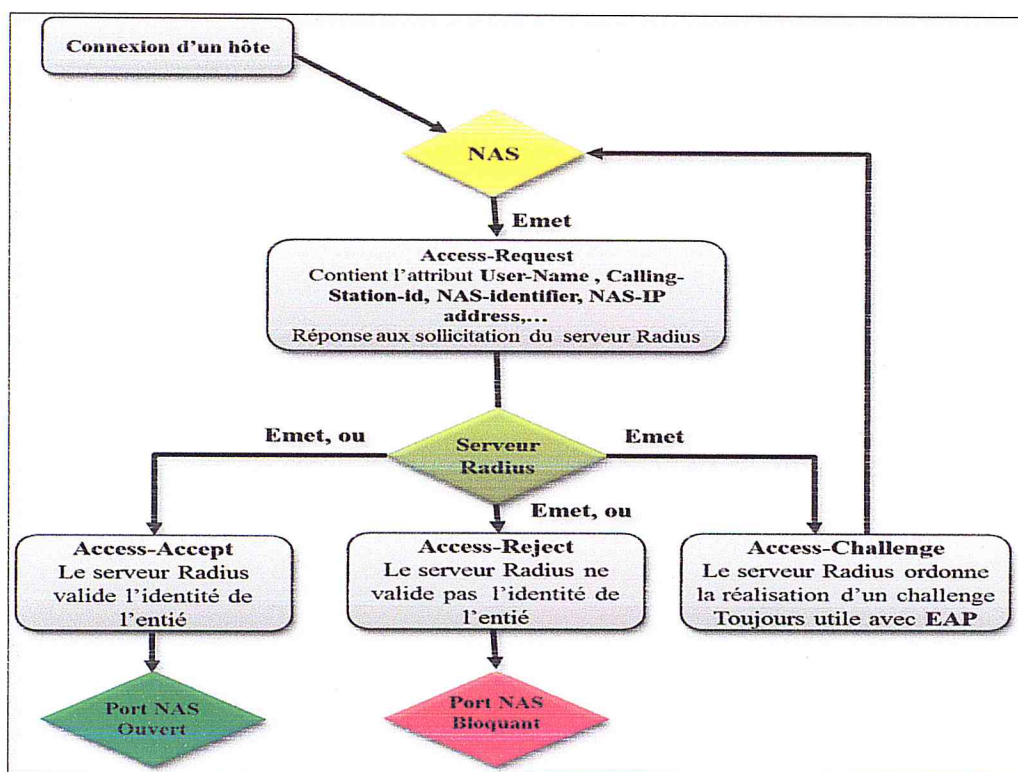


Figure II.08: Organigramme du fonctionnement RADIUS

#### 4.3.4.Format des paquets

Les données sont échangées entre un client et le serveur en paquets RADIUS. En fait, un paquet RADIUS est encapsulé dans un paquet UDP.

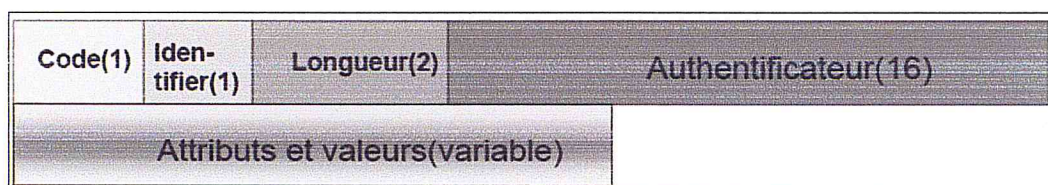


Figure II.09: Format d'un paquet RADIUS

Les champs d'un paquet RADIUS sont les suivants :

Champs	Taille	Usage	Note
<b>Code</b>	<b>1</b>	Type de paquet : <ul style="list-style-type: none"> <li>- Access-Request (code 1)</li> <li>- Access-Accept (code 2)</li> <li>- Access-Reject (code 3)</li> <li>- Access-Challenge (code 11)</li> <li>- Accounting-Request (code 4)</li> </ul>	Défini par la RFC3575
<b>ID</b>	<b>1</b>	ID de session pour associer les requêtes et les réponses	
<b>Longueur</b>	<b>16</b>	Longueur totale du paquet	
<b>Authentificateur</b>	<b>16</b>	Signature du paquet, elle est utilisée par le serveur. Elle est calculée par une fonction MD5 entre les autres champs et un secret partagé.	
<b>Attributs</b>	<b>Var</b>	Variables et leur valeur échangée par l'intermédiaire du protocole.	

Tableau II.01: Eléments d'un message RADIUS

#### 4.3.5. Protocole 802.1X

Le protocole 802.1X est une solution standard lié à la sécurité des réseaux informatiques, mis au point en 2001 par l'IEEE, aussi appelé « Port-Based Network Access Control (PBNAC) », qui a pour objectif la vérification de l'authentification avant la connexion de l'ordinateur au réseau filaire ou non-filaire. En effet, 802.1X travaille au niveau de la couche

2 du modèle OSI et ne requiert pas l'utilisation de la couche 3 (couche IP). Le protocole 802.1X est constitué de trois composants pour le contrôle du port.

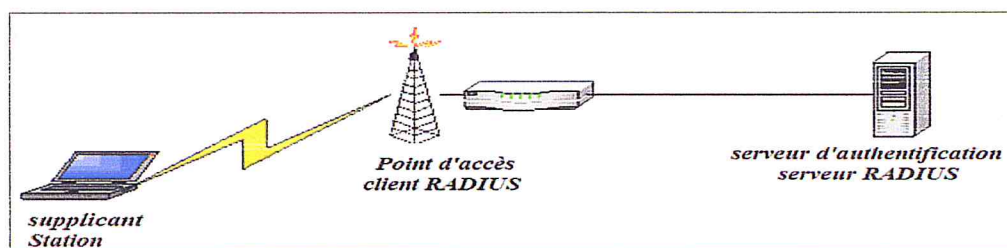


Figure II.10: Architecture d'authentification 802.1X

- **Le demandeur (Supplicant)** : est l'entité qui demande l'accès au réseau via la supplication. C'est le système à authentifier.
- **L'authentificateur (authenticator)** : C'est l'intermédiaire entre le demandeur et le serveur. C'est un élément actif qui met en œuvre le processus d'ouverture ou de fermeture de l'accès au réseau, en fonction de la réponse du serveur d'authentification.
- **Le serveur d'authentification**: Répond aux requêtes de l'authentificateur, en lui indiquant si le demandeur peut se connecter ou non (serveur RADIUS).

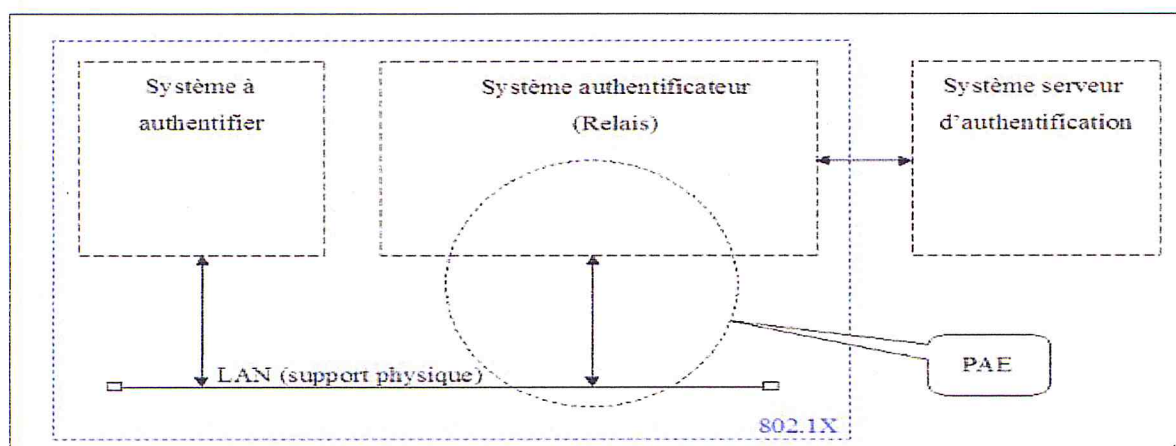


Figure II.11: Les trois entités qui interagissent dans 802.1X

#### 4.3.6. Le point d'accès au réseau (PAE)

La principale innovation amenée par le standard 802.1X consiste à scinder le port d'accès physique au réseau en deux ports logiques, qui sont connectés en parallèle sur le port physique. Le premier port logique est dit « contrôlé », et peut prendre deux états « ouvert » ou

« fermé ». Le deuxième port logique est, lui, toujours accessible mais il ne gère que les trames spécifiques à 802.1X

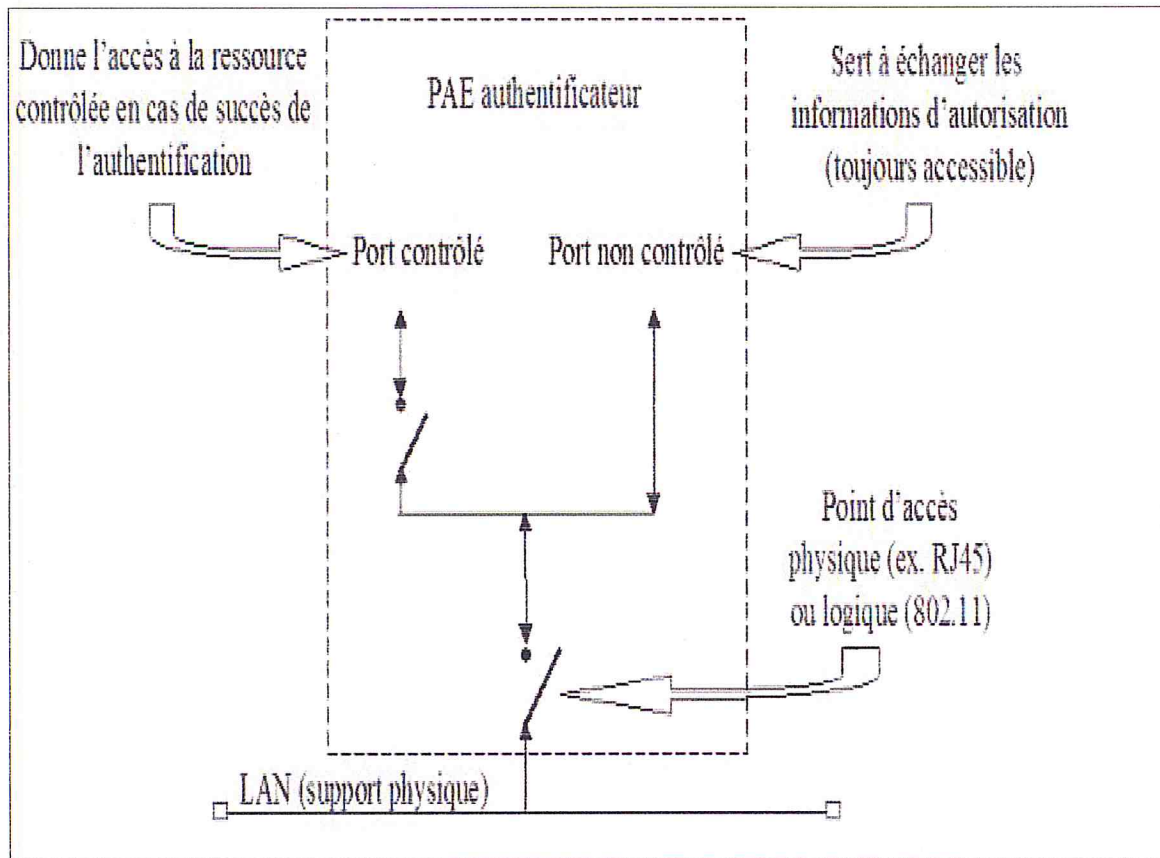
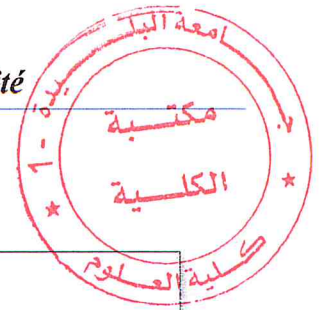


Figure II.12: La structure d'un port dans 802.1x (PAE)



#### 4.3.7.L'architecture proposée

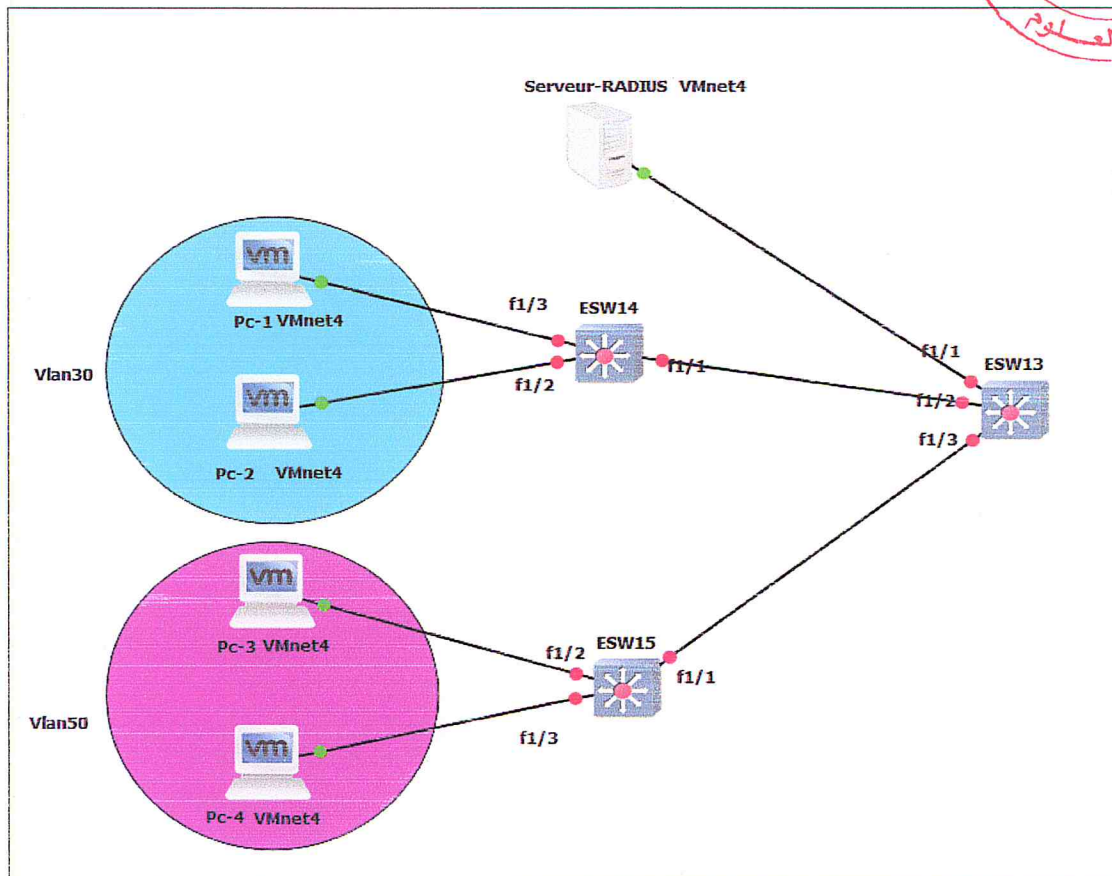


Figure II.13: Architecture du réseau interne (partie utilisateurs)

#### 4.3.8.Choix du mécanisme d'Authentification

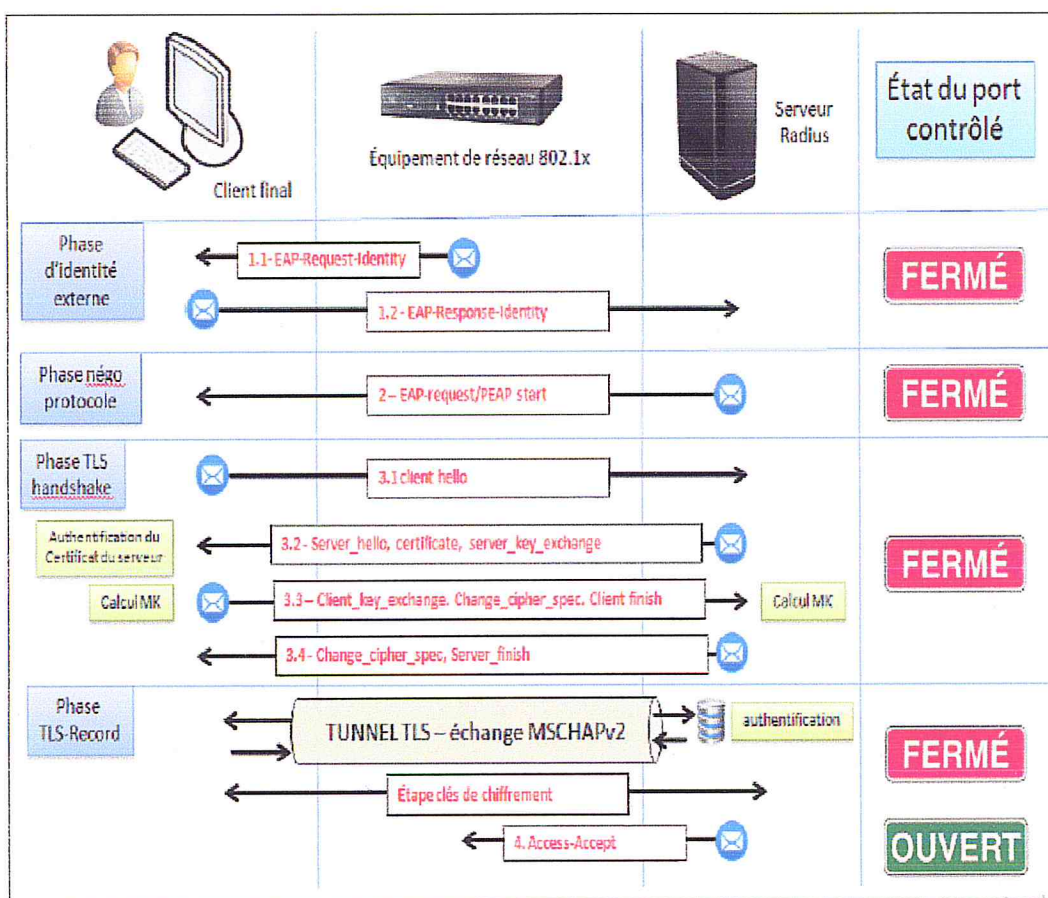
Nous allons utiliser PEAP comme mécanisme d'authentification (certificat coté serveur).

PEAP est un protocole qui a été développé par Microsoft, Cisco et RSA security pour pallier le principal problème d'EAP/TLS, à savoir la nécessité de distribuer des certificats à tous les utilisateurs ou machines. Cela peut être une charge importante, voire ingérable pour certains sites.

Comme avec EAP/TLS, c'est une authentification mutuelle qui s'établit entre le supplicant et le serveur. Mais cette fois, elle est asymétrique. Le serveur sera authentifié par son certificat auprès du supplicant qui, lui-même, s'authentifiera auprès du serveur par la présentation d'un identifiant et d'un mot de passe.

Seul le serveur a besoin d'un certificat. Mais les clients doivent tout de même installer le certificat de l'autorité qui a émis le certificat du serveur. Cela permet de s'assurer que les mots de passe sont envoyés au bon serveur et non à un usurpateur. Comme un mot de passe va être envoyé par le supplicant au serveur, il faudra bien que ce dernier le valide en fonction d'une base d'authentification qu'il pourra interroger. Le serveur Radius devra donc être paramétré de manière à pouvoir valider le mot de passe. En principe, si on décide d'utiliser PEAP, cela signifie que cette base existe déjà sur le site. En général, il s'agit d'une base Windows mais il est aussi possible d'utiliser une base LDAP.

### 4.3.9. Fonctionnement d'PEAP



**Figure II.14: Diagramme d'échanges PEAP**

- **Étape 1 : Identité externe**
  - L'équipement demande au client final de décliner son identité (trame EAPRequest-Identity) ;



- Le client répond par une trame EAP contenant son nom d'utilisateur (trame EAP Réponse-Identity). Ça tombe bien, les trames EAP sont les seules autorisées à entrer dans l'équipement ;
- L'équipement fabrique un paquet IP [access-request] encapsulant la trame [EAP-response-Identity]. Il ajoute d'autres informations comme l'adresse MAC du client final. Ce paquet IP est envoyé au serveur RADIUS.
- **Étape 2 : Négociation de protocole**
  - Le serveur RADIUS reçoit le paquet [Access-Request] et fabrique un paquet [Access challenge] encapsulant une trame [EAP-Request] contenant une proposition de protocole d'identification, comme PEAP.
  - L'équipement décapsule le paquet pour transmettre la trame EAP au client final.
  - Le client final répond dans une trame [EAP-response] transmis de la même manière-indirecte par encapsulation - au serveur RADIUS.
  - Le client et le serveur étant tombés d'accord sur le protocole d'authentification,
- **Étape 3 : TLS handshake**
  - Le serveur RADIUS envoie au client une requête de démarrage [PEAP-START] toujours par le mécanisme d'encapsulation d'une trame EAP. Le client final répond par un message [client hello] avec la liste des algorithmes de chiffrement qu'il connaît.
  - Le serveur envoie son choix d'algorithme, ainsi que son certificat et sa clé publique au client final. Le client final authentifie le serveur. Il génère une « pré-master-Key » avec la clé publique du serveur.
  - Le serveur fait de même et un tunnel chiffré est établi entre eux.
  - Le tunnel sert à protéger l'échange du mot de passe par rapport à une authentification EAP simple.
- **Étape 4 : TLS record**
  - Les échanges liés au protocole de validation du mot de passe vont être effectués dans le tunnel TLS. Avec MSCHAP-V2.
  - Le port s'ouvre lorsque le serveur envoie au client final un message [Access-Accept] après avoir vérifié le mot de passe de l'utilisateur et s'être assuré de ses autorisations.

### **Conclusion**

Dans ce chapitre, nous avons étudié une solution parmi les solutions proposées dans la littérature pour l'interconnexion des deux sites distants de l'entreprise et l'accès distant sécurisé afin de permettre à des utilisateurs itinérants d'accéder au réseau d'entreprise, les protocoles implémentés pour véhiculer les données de l'entreprise de manière sûre et fiable (redondance), Radius pour l'authentification PEAP, Proxy pour le filtrage URL et l'accès au page WEB plus rapide.

Le chapitre suivant va comporter les étapes de l'implémentation de notre solution de sécurité dans un environnement virtuel similaire au réseau informatique de notre organisme d'accueil, le choix d'utiliser un environnement virtuel a été imposé par la société pour des raisons de confidentialité.

# Chapitre III

### Introduction

Cette partie présente en détail la mise en œuvre de la simulation de notre réseau basé sur les technologies suivantes: VPN site to site, VPN d'accès distant, proxy et filtrage URL, redondance pour le Datacenter (HSRP, GLBP, Failover, Etherchannel, Spanning tree), Authentification PEAP, NAT.

Ce chapitre se compose de trois principales parties. Dans la première partie, nous donnons un aperçu des outils choisis pour réaliser la simulation. Dans la deuxième partie, nous montrons les différentes configurations mises en place au cours de notre simulation. La dernière partie est une description des tests effectués sur notre réseau.

### 1. Supports et logiciel de tests

Cette phase de test et de réalisation a nécessité l'utilisation de plusieurs logiciels de simulation et d'émulation de réseau, lesquels seront présentés dans ce qui suit:

#### 1.1 Présentation de GNS3

GNS3 est un outil libre de simulation de réseau. Il permet de simuler des équipements Cisco et l'intégration des machines virtuelles.

Contrairement à d'autres outils, GNS3 permet de choisir les équipements à simuler.

L'outil utilise de vraies images de système d'exploitation, ce qui offre des conditions plus réalistes de simulation.

L'outil est doté d'une interface graphique facile d'utilisation. Il offre un espace de travail qui permet de mettre en place la topologie réseau à simuler.

## Chapitre III : Implémentation

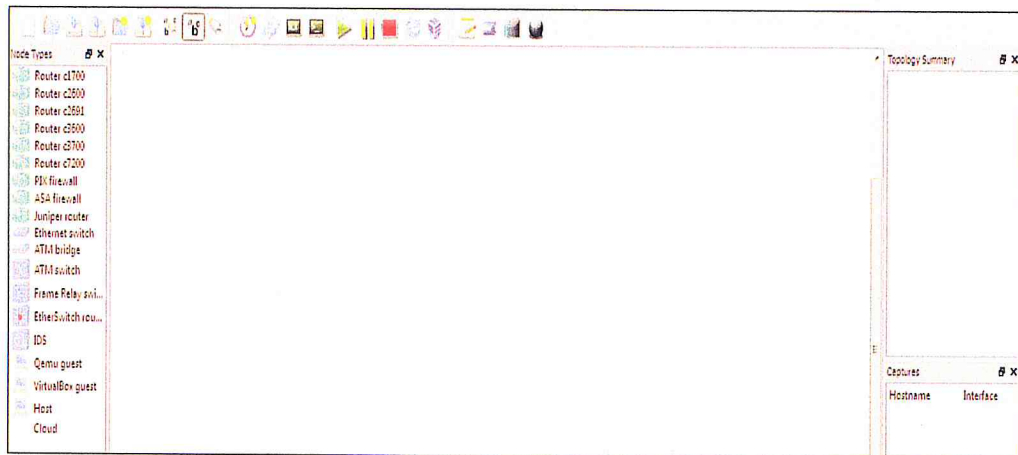


Figure III.01 : Interface graphique de l'émulateur GNS3

### 1.2 Présentation de VMware Workstation

VMware Workstation est un logiciel de virtualisation de PC pour les développeurs de logiciels et les professionnels. Il permet de faire fonctionner simultanément plusieurs systèmes d'exploitation sur un seul PC. Nous pourrions ainsi disposer de machines Windows, linux en même temps, avec une seule machine physique. Ces machines pourront être parfaitement intégrées à notre réseau.

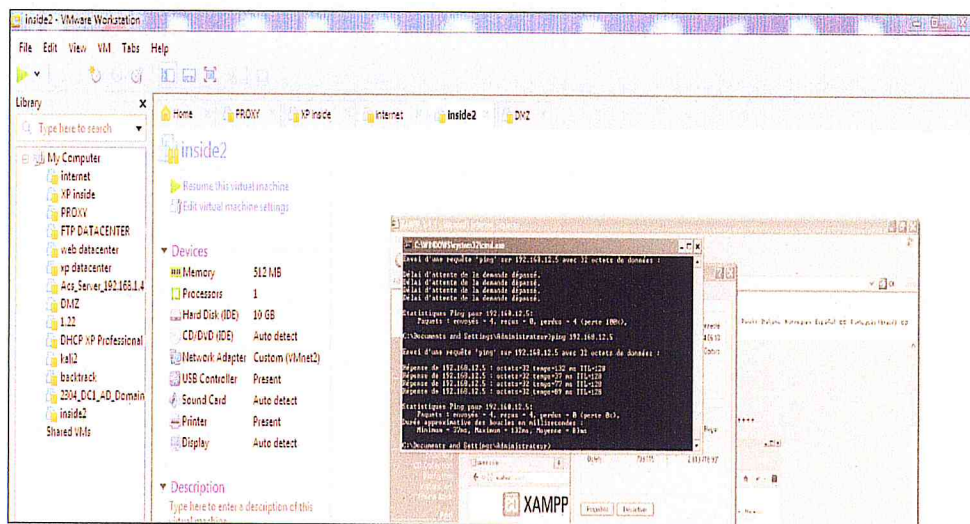


Figure III.02 : Interface de VMware Workstation

## 2. Les configurations mise en place

### 2.1. Partie passerelle internet

#### 2.1.1. Présentation de l'architecture

Notre architecture est constituée des actifs suivants (voir **figure IV.03**)

- cinq (6) machine virtuelles:
  - Une machine pour simuler le serveur http (web) du DMZ
  - Une machine pour simuler ordinateur client du réseau Inside de SITE Groupe SAIDAL (Windows xp)
  - Une machine pour simuler ordinateur client du réseau Inside de site de Blida (Windows xp)
  - Une machine pour simuler ordinateur du réseau d'internet (Windows xp)
  - Une machine pour simuler proxy ISA serveur (Serveur 2003)
- Deux firewalls ASA: ASA-3 pour site Groupe SAIDAL et ASA-4 pour le site de Blida
- Deux routeur : R2 et router FAI pour le réseau internet

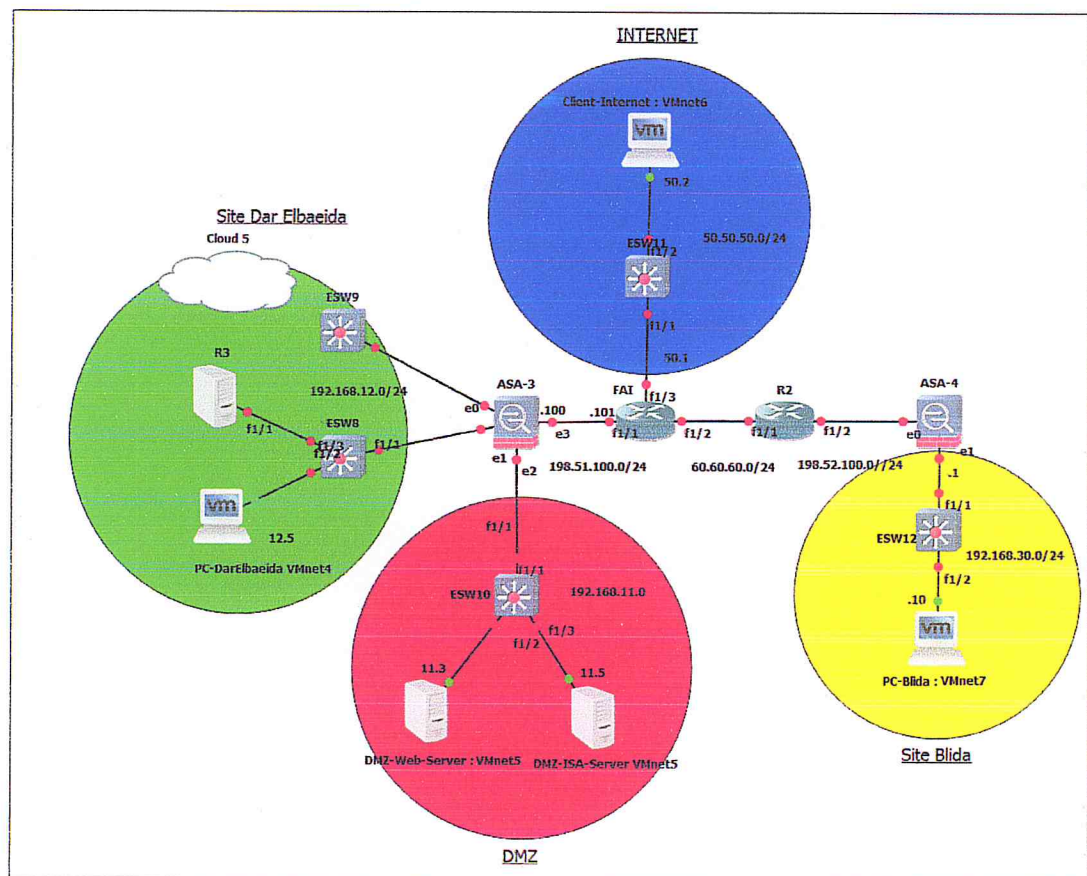


Figure III.03 : l'architecture proposée (partie passerelle Internet)

2.1.2. L'adressage

SITE	Adresse réseaux
SITE GROUPE SAIDAL	192.168.12.0/24
SITE BLIDA	192.168.30.0/24

Tableau III.01 : le plan d'adressage des sites de Groupe SAIDAL et de Blida

Matérielle	Interface	Adresse IP	Masque	
Routeur FAI	Fa1/2	60.60.60.1	255.255.255.0	
	Fa1/3	50.50.50.1	255.255.255.0	
	Fa1/1	198.51.100.101	255.255.255.0	
Routeur 2	Fa1/1	60.60.60.2	255.255.255.0	
	Fa1/2	198.52.100.1	255.255.255.0	
ASA-3	Ethernet2	192.168.11.1	255.255.255.0	
	Ethernet1	192.168.12.1	255.255.255.0	
	Ethernet3	198.51.100.100	255.255.255.0	
ASA-4	Ethernet0	198.52.100.2	255.255.255.0	
	Ethernet1	192.168.30.1	255.255.255.0	
DMZ-ISA-SERVER		192.168.11.5	255.255.255.0	
DMZ-Web-SERVER		192.168.11.3	255.255.255.0	
Client-Internet		50.50.50.2	255.255.255.0	
Pc-Dar El-Beida		192.168.12.5	255.255.255.0	

Pc-Blida		192.168.30.10	255.255.255.0	
----------	--	---------------	---------------	--

**Tableau III.02 : l'adressage des sites de Groupe SAIDAL et de Blida**

### **2.1.3. Les configurations**

#### **2.1.3.1. Configuration des routeurs R2 et FAI**

Pour chaque routeur nous devons configurer : les interfaces et le routage

La configuration du routeur R2 et FAI est présentée dans l'Annexe 1

#### **2.1.3.2. Configuration des pare-feux**

##### **2.1.3.2.1. pare-feu ASA-3**

- Les interfaces (inside, outside, DMZ)
- NAT dynamique : les utilisateurs de réseau inside accèdent à l'internet via une adresse publique entre 198.51.100.50 et 198.51.100.61
- NAT statique: les clients internet accèdent au serveur web avec adresse publique 198.51.100.14
- VPN site to SITE: VPN Ipsec entre site Groupe SAIDAL et site Blida (AES, SHA)
- VPN Remote Access:
- routage :
- ACL: vont se résumer en une liste d'adresse ou de ports autorisés ou interdits par le dispositif de filtrage:
  - autoriser les utilisateurs du réseau inside d'accéder au service du dmz (HTTP) et au réseau internet
  - autoriser les utilisateurs du réseau internet d'accéder au service du dmz (HTTP).

La configuration du firewall ASA-3 est présentée dans l'Annexe 2

##### **2.1.3.2.2. Pare-feu ASA-4**

Nous devons configurer :

- ✓ Routage
- ✓ VPN site to site



La configuration du firewall ASA-4 est présentée dans l'Annexe 3

### 2.1.3.3. Configuration du proxy ISA serveur:

Configuration de la mise en cache:

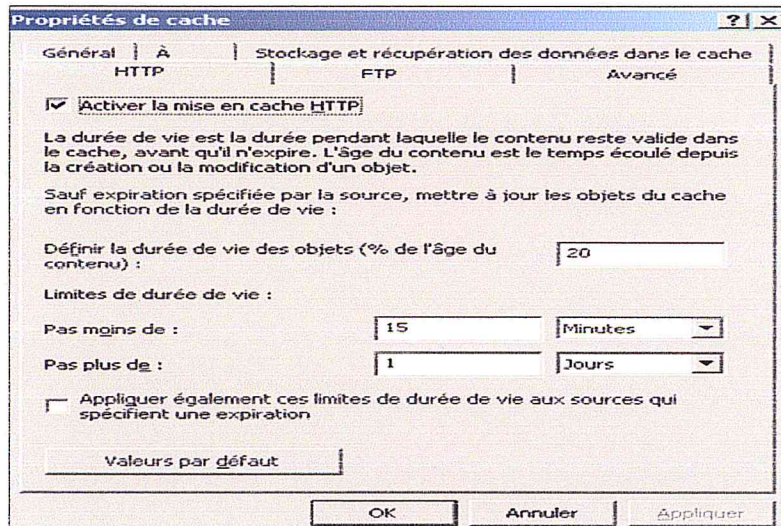


Figure III.04: les propriétés de mise en cache d'ISA Server

Filtrage URL:



Figure III .05 : le filtrage url dans ISA Server

Blacklist: La liste noire représente l'ensemble des sites interdits pour les utilisateurs de l'entreprise

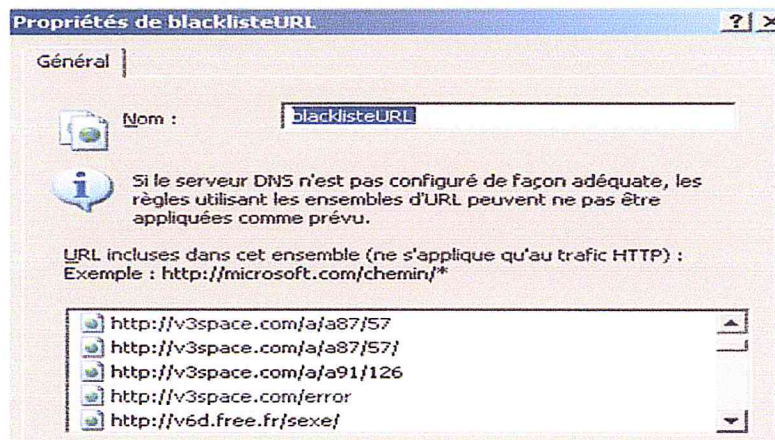


Figure III.06 : les propriétés de blacklistURL dans ISA Server

## 2.2. Partie Datacenter

### 2.2.1. Présentation de l'architecture

Notre architecture est constituée des actifs suivants (voir Figure III.04)

- Trois (4) machine virtuelles:
  - ✓ Une machine pour simuler le serveur http (web)
  - ✓ Deux machines pour simuler ordinateur client du réseau Inside de SITE Groupe SAIDAL (Windows xp)
  - ✓ Une machine pour simuler le serveur de fichier (ftp)
- Deux firewalls ASA: les firewalls ASA-1 et ASA-2 configurés en mode actif/standby
- Deux Switch core (ESW1 et ESW2), deux Switch Access (ESW3 et ESW4), routeur DHCP.

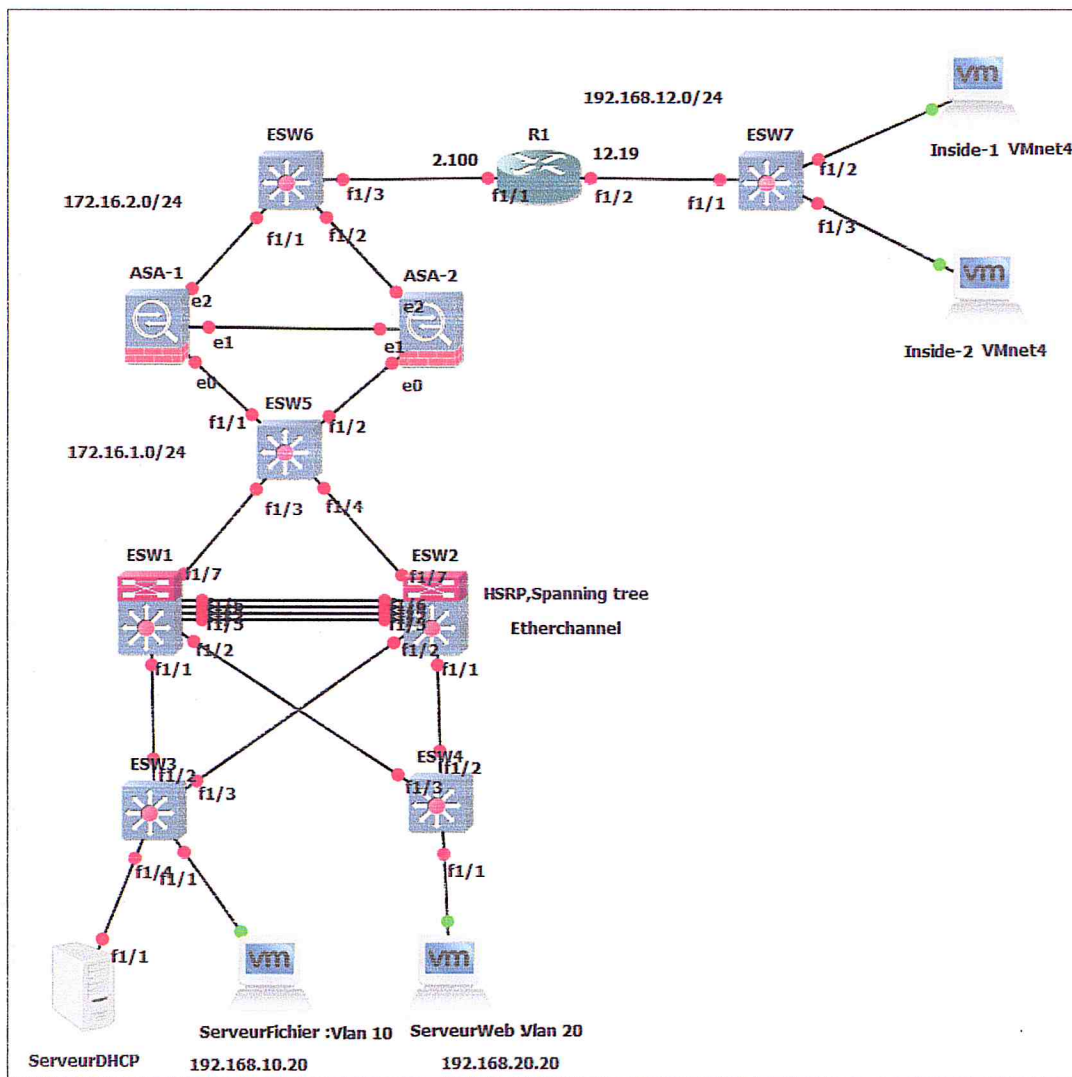


Figure III.07: l'architecture proposée (partie Data Center)

### 2.2.2. L'adressage

Vlan	Adresse
Vlan 10	192.168.10.0/24
Vlan 20	192.168.20.0/24

Tableau III.08 : le plan d'adressage des vlans (partie Data Center)

Matérielle	Interface	Adresse
<b>Routeur 1</b>	<b>FastEthernet0/0</b>	<b>172.16.2.100/24</b>
	<b>FastEthernet0/1</b>	<b>192.168.12.19/24</b>
<b>ASA-1</b>	<b>Ethernet 0</b>	<b>172.16.1.1</b>
	<b>Ethernet 1</b>	<b>172.16.2.1</b>
	<b>Ethernet 2</b>	<b>10.1.0.1</b>
<b>SERVEUR WEB</b>		<b>192.168.2.1</b>
<b>SERVEUR FTP</b>		<b>192.168.1.1</b>

Tableau III.04 : l'adressage des vlans (partie Data Center)

### 2.2.3. Les configurations

#### 2.2.3.1. Configuration des Switch core ESW1 et ESW2 (niveau 3) :

La configuration des commutateurs niveau 3 ESW1 et ESW2 est présenté dans l'Annexe 4, pour chaque commutateur nous devons configurer: **Routage, failover, Etherchannel, Spanning tree** routage inter-vlan.

HRSP pour le Switch ESW1 Actif pour vlan 10 et standby pour le vlan 20, le Switch ESW2 actif pour vlan 20 et standby pour vlan 10

GLBP pour le Switch ESW1 Actif pour vlan 10 et standby pour le vlan 20, le Switch ESW2 actif pour vlan 20 et standby pour vlan 10

#### 2.2.3.2. Les firewalls ASA-1et ASA-2

Nous devons configurer: protocole failover (actif, standby), routage, ACL.

ACL: pour autoriser les utilisateurs de l'entreprise d'accéder aux services du Datacenter tel que: DHCP, HTTP, FTP, HTTPS.

La configuration des firewalls ASA3 et ASA4 est présenté dans l'Annexe 5.

### 2.2.3.3. Les Switch ESW3 et ESW4:

Nous devons configurer les vlan et DHCP Snooping

### 2.2.3.4. Configuration du proxy ISA serveur:

Configuration de la mise en cache:

## 2.3. La partie Authentification RADIUS

### 2.3.1. L'architecture proposée

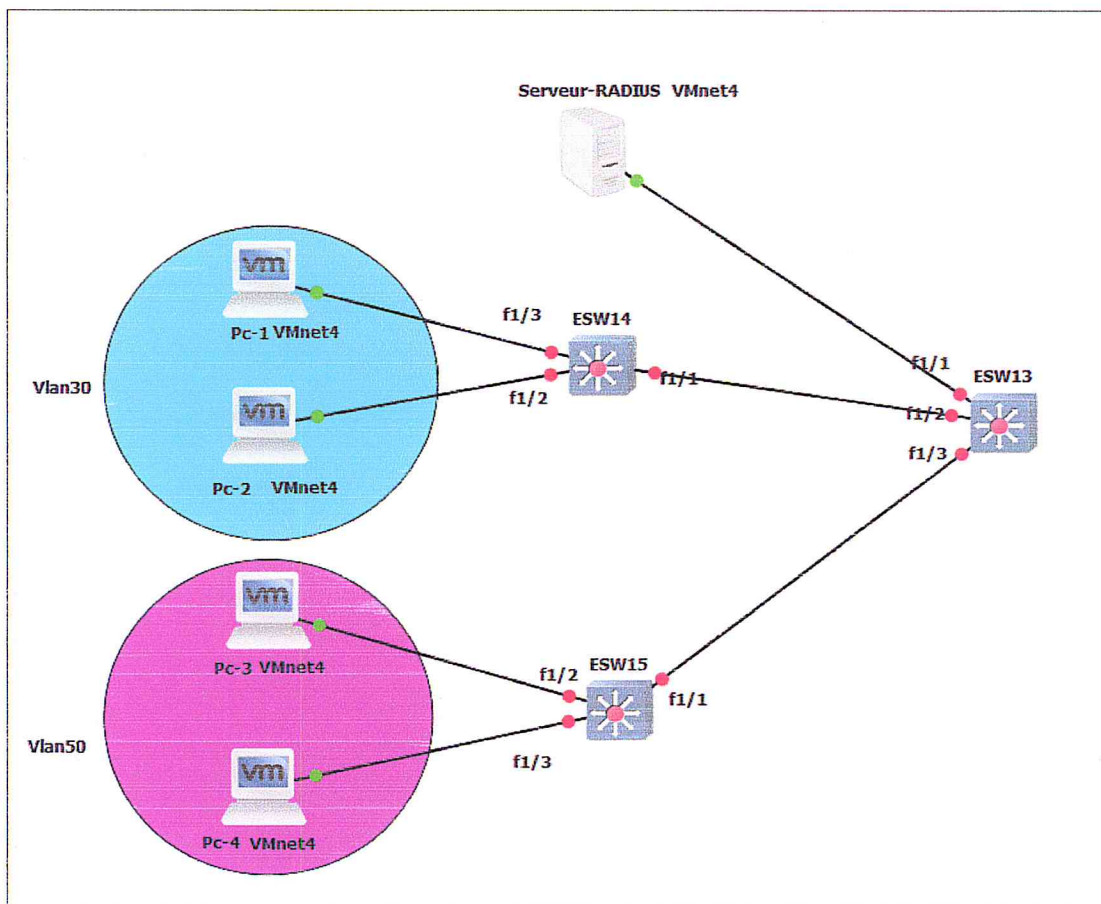


Figure III.09 : l'architecture du réseau interne LAN

### 2.3.1. Les configurations

#### 2.3.1.1. Installation de serveur contrôleur de domaine

Nous avons créé un contrôleur de domaine pour le domaine « **gs.est** », nom choisi arbitrairement à titre d'exemple. Ce serveur fait également office de serveur DNS et de global catalogue (annuaire d'objets Active Directory).

La première étape est d'installer le système d'exploitation, Windows Server 2012 R2, sur une nouvelle machine virtuelle (**VMware workstation**). Cette machine possède une interface réseau virtuelle qui est configuré pour se comporter comme une interface réseau physique.

La deuxième étape consiste à installer **Active Directory** et le service **DNS**. Pour cela, il faut exécuter `promote This server to a Domain Controller` et suivre l'assistant pas à pas

- Créer un nouveau domaine dans une nouvelle forêt;
- Configurer le contrôleur de domaine comme serveur DNS;
- Définir un mot de passe de restauration et redémarrer quand cela est demandé.

### 2.3.1.2. Mise en place d'une plate-forme PKI

Pour pouvoir utiliser une authentification sécurisée avec PEAP, NPS le (*Network Policy Server*) a besoin d'un certificat qu'il puisse envoyer aux clients. Ce certificat doit être délivré par une autorité de confiance, en l'occurrence notre contrôleur de domaine. Pour faire de notre contrôleur de domaine une autorité de certification, il faut lui ajouter le rôle « **Active Directory Certificat Services** » avec les options par défaut.

La procédure d'installation de la plate-forme de gestion de clé PKI. Dans cette partie nous allons présenter les différentes étapes nécessaires pour la mise en place d'une plate-forme de gestion de clé PKI, ceci va nous permettre de générer des certificats conformes à la norme X509, pour les différents clients afin de renforcer le processus d'authentification. Pour cela nous allons utiliser Windows server 2012 R2

### 2.3.1.3. Installation du NPS (Network Policy Server)

Le serveur NPS nous permet de créer et de mettre en œuvre des stratégies d'accès réseau à l'échelle d'une entreprise pour assurer l'intégrité des clients, l'authentification des demandes de connexion et l'autorisation des demandes de connexion.

Par défaut, NPS écoute le trafic RADIUS sur les ports 1812, 1813 1645, et 1646 sur toutes les cartes réseau installées. Si nos serveurs d'accès au réseau sont configurés pour envoyer du trafic RADIUS sur les ports autres que ces valeurs par défaut, on doit supprimer les exceptions créées dans le pare-feu Windows avec sécurité avancée lors de l'installation de NPS et créer les exceptions pour les ports qui seront utilisés pour le trafic RADIUS.

Pour installer un Serveur-RADIUS sur Windows server 2012, il faut d'abord installer le NPS.

Une fois le rôle est bien installé, il faut dans un premier temps rajouter les différents clients RADIUS (Switch, points d'accès, etc...) sur le serveur .C'est ensuite qu'on pourra configurer nos « Stratégies réseau ». Il est important de noter que les stratégies réseaux suivent un ordre de traitement. Dans notre cas, nous avons défini une stratégie pour l'accès aux réseaux filaires AAA. En effet, on peut créer plusieurs stratégies selon le besoin et chaque stratégie dispose d'un numéro de traitement spécifique qui permettra de les traiter de manière croissante. Cela veut dire que notre serveur RADIUS va évaluer chaque stratégie et appliquer les paramètres relatifs à celle (la stratégie) qui aura remplies toutes les conditions.

### 2.3.1.4. Comptabilisation NPS

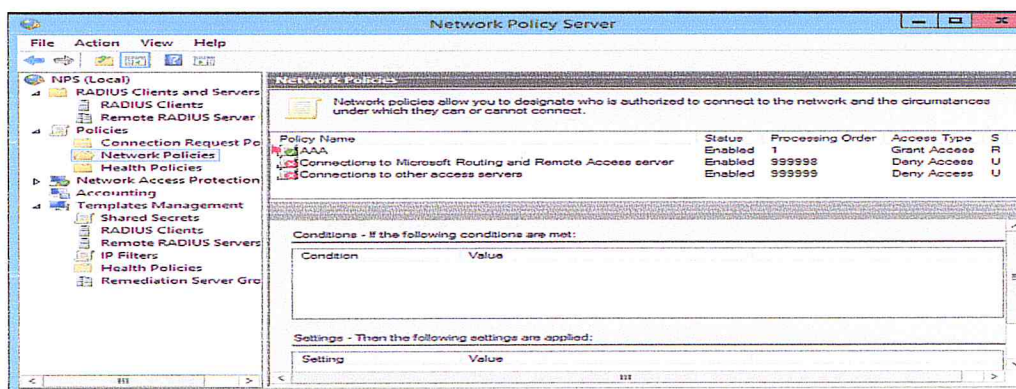


Figure III.10: Comptabilisation NPS

On peut configurer *NPS* (*Network Policy Server*) de façon à gérer les comptes RADIUS pour les demandes d'authentification utilisateur, les messages d'acceptation et de refus d'accès, les demandes et les réponses de gestion des comptes ainsi que les mises à jour périodiques de l'état. Par ailleurs, on peut utiliser cette procédure pour configurer les propriétés de journalisation et la connexion au serveur exécutant SQL Server qui héberge vos données de gestion. À l'aide des journaux d'événements de l'Observateur d'événements, on peut analyser les erreurs *NPS* et les autres événements dont on a configuré l'enregistrement par *NPS*.

Le *NPS* enregistre les événements d'échec d'une demande de connexion dans les journaux d'événements Système et Sécurité par défaut. Ces événements d'échec consistent en demandes rejetées ou ignorées par le *NPS*. D'autres événements d'authentification *NPS* sont

enregistrés dans le journal système de l'Observateur d'événements en fonction des paramètres qu'on spécifie dans le composant logiciel enfichable *NPS*. Certains événements susceptibles de contenir des données sensibles sont enregistrés dans le journal de la sécurité de l'Observateur d'événements. Le *NPS* permet aussi de garder une traçabilité des utilisateurs en stockant un historique de leur passage sur le réseau.

### 2.3.1.5. Les clients RADIUS

Les clients RADIUS sont des commutateurs compatibles avec la norme 802.1X, configurés comme des clients sur le service *NPS*. Le Switch d'accès est un transporteur d'informations d'authentification jusqu'au serveur, il attend ensuite la réponse pour savoir comment agir et quelles autorisations attribuer au client.

La configuration des clients Radius nécessite les étapes suivantes :

- une configuration initiale sur le commutateur d'accès tel que les mots de passe d'accès.
- La création des vlan.
- L'affectation des ports de connexion aux vlans de travail.
- Configuration des Service AAA.
- Configuration des ports.

### 2.3.1.6. Configuration du poste client « Supplicant »

Le client est un ordinateur sous Windows, qui dispose d'une connexion filaire Ethernet et qui désire accéder aux ressources internes du réseau filaire. La première étape consiste à joindre le client au domaine Active Directory et la deuxième étape consiste le déploiement du certificat au client. La dernière étape est de configurer la connexion au réseau filaire de l'ordinateur pour l'authentification (voir l'annexe 6)

## 3. Test sur le réseau

### 3.1. TEST de VPN entre site Groupe SAIDAL et site de Blida:

Nous allons tester notre configuration en faisant un Ping sur les machines distantes.



```
Command Prompt
C:\Documents and Settings\Administrator>ping 192.168.30.10
Pinging 192.168.30.10 with 32 bytes of data:
Reply from 192.168.30.10: bytes=32 time=176ms TTL=128
Reply from 192.168.30.10: bytes=32 time=54ms TTL=128
Reply from 192.168.30.10: bytes=32 time=37ms TTL=128
Reply from 192.168.30.10: bytes=32 time=60ms TTL=128

Ping statistics for 192.168.30.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 37ms, Maximum = 176ms, Average = 81ms

C:\Documents and Settings\Administrator>
```

Figure III.11 : Test de connectivité depuis le Site Groupe SAIDAL vers le site Blida

L'encadré rouge indique que le test effectué à partir d'un poste utilisateur qui se trouve au niveau du site Groupe SAIDAL vers un autre poste utilisateur qui se situe au niveau du site Blida (encadré vert). Le résultat de la commande est présenté par L'encadré bleu. Nous remarquons ici que le test de connectivité entre les deux sites a réussi.

```
Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Administrator>ping 192.168.12.5
Pinging 192.168.12.5 with 32 bytes of data:
Reply from 192.168.12.5: bytes=32 time=137ms TTL=128
Reply from 192.168.12.5: bytes=32 time=60ms TTL=128
Reply from 192.168.12.5: bytes=32 time=142ms TTL=128
Reply from 192.168.12.5: bytes=32 time=58ms TTL=128

Ping statistics for 192.168.12.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 58ms, Maximum = 142ms, Average = 99ms

C:\Documents and Settings\Administrator>
```

Figure III.12: Test de connectivité depuis le site Blida vers le site Groupe SAIDAL

Même test au niveau du site de Blida et le résultat démontre qu'il a réussi

Nous pouvons voir dans la Figure III.09 que le tunnel créer est actif en utilisant la commande (show crypto ipsec stats), l'état du tunnel est actif (encadré vert).

```
ciscoasa# show crypto ipsec stats
IPsec Global Statistics
-----
Active tunnels: 1
Previous tunnels: 1
Inbound
  Bytes: 0
  Decompressed bytes: 0
  Packets: 12
  Dropped packets: 0
  Replay failures: 0
  Authentications: 12
  Authentication failures: 0
  Decryptions: 12
```

Figure III.13 : Etat du tunnel VPN site to site

### 3.2 Test de VPN Remote Access

L'utilisateur du réseau internet tape son nom et son mot de passe pour connecté à l'entreprise

### Chapitre III : Implémentation

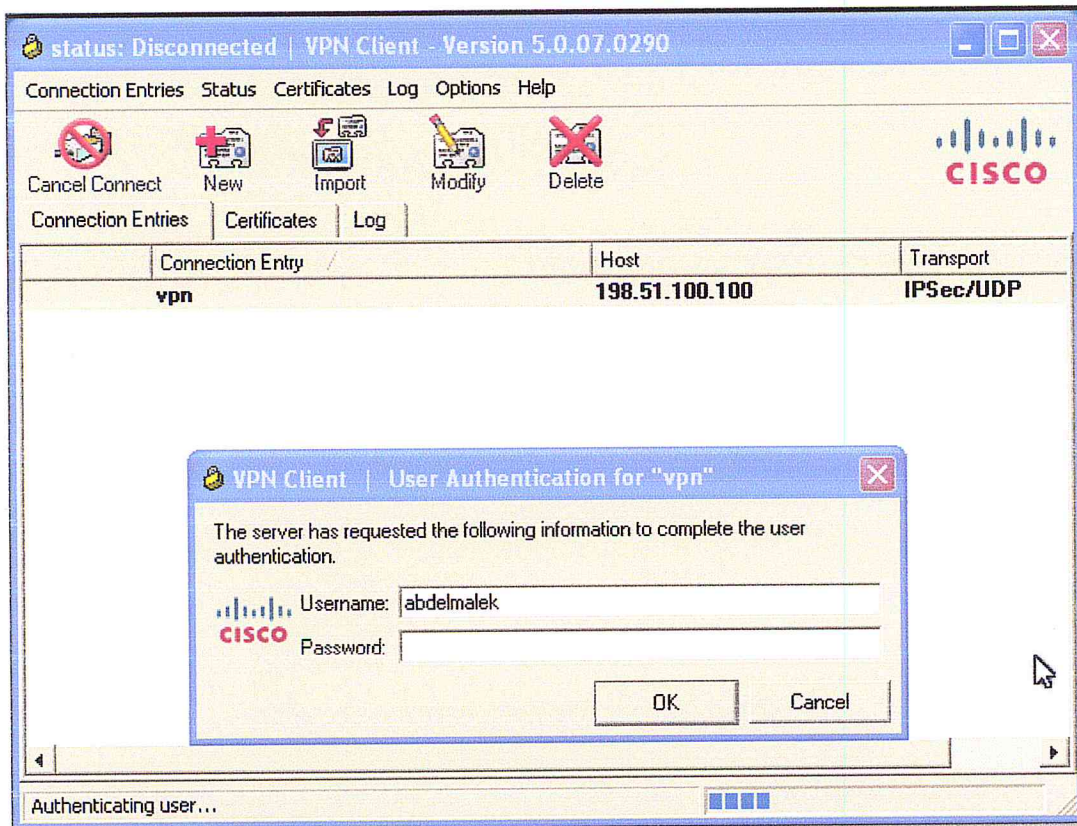


Figure III.14 : test de VPN Access

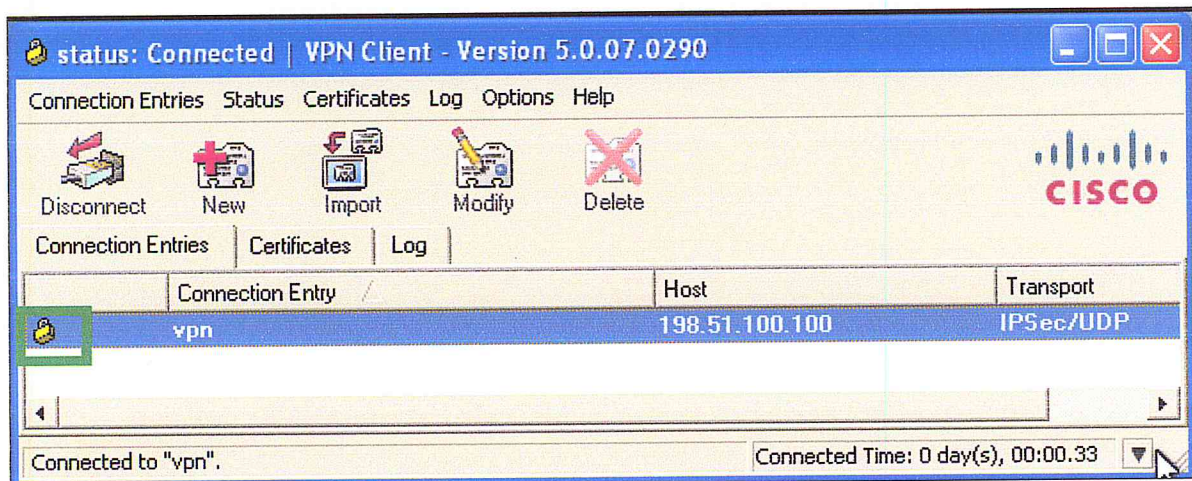


Figure III.15 : test de VPN Access

Le résultat démontre que l'utilisateur a réussi de connecté à l'entreprise (l'encadré vert)

Nous pouvons voir dans la Figure III.12 le tunnel créé est actif en utilisant la commande (show crypto ipsec stats), l'état du tunnel est actif (encadré vert).

```
ciscoasa# show ipsec stats

IPsec Global Statistics
-----
Active tunnels: 2
Previous tunnels: 2
Inbound
  Bytes: 0
  Decompressed bytes: 0
  Packets: 12
  Dropped packets: 0
  Replay failures: 0
  Authentications: 12
```

**Figure III.16 : état de VPN**

Dans la figure on voit qu'il y a 2 tunnels active (vpn site to site et vpn remote access)  
L'administrateur de l'entreprise utilise le VPN remotes access pour accéder au réseau interne de l'entreprise pour configurer n'importe quel équipement de son domicile

```
ASA Version 8.4(2)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0
 nameif inside
 security-level 100
 ip address 192.168.12.1 255.255.255.0
!
interface GigabitEthernet1
 nameif DMZ
 security-level 50
 ip address 192.168.11.1 255.255.255.0
!
interface GigabitEthernet2
 nameif outside
 security-level 0
 ip address 198.51.100.100 255.255.255.0
!
```

**Figure III.17: Configuration de Parfeu ASA1**

Le résultat montre que l'administrateur a réussi d'accéder au parfeu ASA1 qui se trouve dans le réseau interne de l'entreprise

### 3.3 Test de NAT

```
nat: translation - any:192.168.12.5/512 to any:198.51.100.58/512
nat: translation - any:192.168.12.5/512 to any:198.51.100.58/512
nat: translation - any:192.168.12.5/512 to any:198.51.100.58/512
nat: translation - any:192.168.12.5/512 to any:198.51.100.58/512
```

Figure III.18: Test de NAT

Le résultat montre que l'utilisateur avec l'adresse privé 192.168.12.5 accède à internet via l'adresse publique 198.51.100.58

### 3.4. Test de Redondance

Pour tester la Redondance de notre architecture (datacenter) il faut débrancher ou éteindre un Switch core ou un des pare-feux.

#### 3.4.1. Cas où il y a pas une panne

Le Switch core ESW1 est actif pour les vlan 10 et standby pour les vlan 20

```
ESW1#show
*Mar 1 00:00:39.959: %HSRP-5-STATECHANGE: Vlan10 Grp 10 state Speak -> Standby
*Mar 1 00:00:39.975: %HSRP-5-STATECHANGE: Vlan20 Grp 20 state Speak -> Standby
*Mar 1 00:00:40.459: %HSRP-5-STATECHANGE: Vlan10 Grp 10 state Standby -> Active
*Mar 1 00:00:40.475: %HSRP-5-STATECHANGE: Vlan20 Grp 20 state Standby -> Active
```

Figure III.19 : L'état du Protocole HSRP pour le switch ESW1

```
S1#
*Mar 1 00:00:37.955: %GLBP-6-STATECHANGE: Vlan10 Grp 1 state Standby -> Active
*Mar 1 00:00:37.959: %GLBP-6-STATECHANGE: Vlan20 Grp 1 state Standby -> Active
```

Figure III.20 : L'état du Protocole GLBP pour le switch S2

Le pare-feu ASA-1 est actif et ASA-2 est standby (l'encadré vert)

```
ciscoasa# show failover
Failover On
Failover unit Primary
Failover LAN Interface: FO GigabitEthernet1 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 2 of 60 maximum
Version: Ours 8.4(2), Mate 8.4(2)
Last Failover at: 13:33:21 UTC Jun 11 2017
This host: Primary - Active
```

Figure III.21: L'état du Protocole failover pour le parefeu ASA-1

```
ciscoasa# sh failover
Failover On
Failover unit Secondary
Failover LAN Interface: FO GigabitEthernet1 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 2 of 60 maximum
Version: Ours 8.4(2), Mate 8.4(2)
Last Failover at: 13:33:12 UTC Jun 11 2017
This host: Secondary - Standby Ready
```

Figure III.22: L'état du Protocole failover pour le parefeu ASA-2

### 3.4.2. Cas de panne de switch ESW1

Le switch ESW2 devient actif pour tous les vlans

```
ESW2#
*Mar 1 00:00:39.387: %HSRP-5-STATECHANGE: Vlan10 Grp 10 state Speak -> Standby
*Mar 1 00:00:39.607: %HSRP-5-STATECHANGE: Vlan20 Grp 20 state Speak -> Standby
*Mar 1 00:00:39.887: %HSRP-5-STATECHANGE: Vlan10 Grp 10 state Standby -> Active
*Mar 1 00:00:40.107: %HSRP-5-STATECHANGE: Vlan20 Grp 20 state Standby -> Active
```

Figure III.23: L'état du Protocole HSRP pour le switch ESW2

### 3.4.3. cas de panne du parefeu ASA-1

Le pare-feu ASA-2 devient actif

```
ciscoasa# sh failover
Failover On
Failover unit Secondary
Failover LAN Interface: FO GigabitEthernet1 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 2 of 60 maximum
Version: Ours 8.4(2), Mate 8.4(2)
Last Failover at: 13:38:57 UTC Jun 11 2017
  This host: Secondary - Active
    Monitor timer: 00 (sec)
      Interface inside (172.16.1.1): Normal (Waiting)
      Interface outside (172.16.2.1): Normal (Waiting)
  Other host: Primary - Failed
    Active time: 315 (sec)
      Interface inside (172.16.1.2): Unknown (Monitored)
      Interface outside (172.16.2.2): Unknown (Monitored)
```

Figure III.24: L'état de parfeu ASA-2

### 3.5. Test de sécurité de protocole hsrp:

#### 3.5.1. Cas ou HSRP n'est pas sécurisé :

Avant l'attaque:

Switch ESW1:

```
ESW1#show
*Mar 1 00:00:39.959: %HSRP-5-STATECHANGE: Vlan10 Grp 10 state Speak -> Standby
*Mar 1 00:00:39.975: %HSRP-5-STATECHANGE: Vlan20 Grp 20 state Speak -> Standby
*Mar 1 00:00:40.459: %HSRP-5-STATECHANGE: Vlan10 Grp 10 state Standby -> Active
*Mar 1 00:00:40.475: %HSRP-5-STATECHANGE: Vlan20 Grp 20 state Standby -> Active
```

Figure III.25: L'état du Protocole HSRP pour le switch ESW1

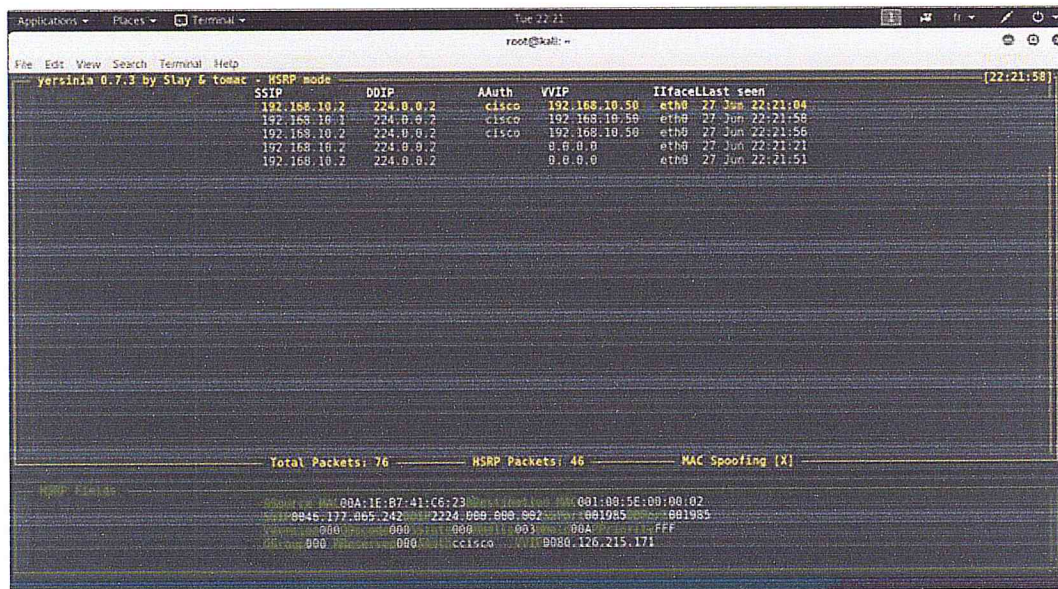
Switch ESW2:

```
ESW2#
*Mar 1 00:00:39.387: %HSRP-5-STATECHANGE: Vlan10 Grp 10 state Speak -> Standby
*Mar 1 00:00:39.607: %HSRP-5-STATECHANGE: Vlan20 Grp 20 state Speak -> Standby
*Mar 1 00:00:39.887: %HSRP-5-STATECHANGE: Vlan10 Grp 10 state Standby -> Active
*Mar 1 00:00:40.107: %HSRP-5-STATECHANGE: Vlan20 Grp 20 state Standby -> Active
```

Figure III.26: L'état du Protocole HSRP pour le switch ESW2

pour attaquer le protocole HSRP il faut utiliser l'outil yersinia (kali ou backtrack)

Attaque HSRP:



```
yersinia 0.7.3 by Slay & tomac - HSRP mode [22:21:58]
SSIP      DDIP      AAuth     VVIP      IifacelLast seen
192.168.10.2 224.0.0.2 cisco     192.168.10.50 eth0 27 Jun 22:21:04
192.168.10.1 224.0.0.2 cisco     192.168.10.50 eth0 27 Jun 22:21:58
192.168.10.2 224.0.0.2 cisco     192.168.10.50 eth0 27 Jun 22:21:56
192.168.10.2 224.0.0.2      0.0.0.0   eth0 27 Jun 22:21:21
192.168.10.2 224.0.0.2      0.0.0.0   eth0 27 Jun 22:21:51

-----
Total Packets: 76      HSRP Packets: 46      MAC Spoofing [X]

HSRP Entries
-----
Source MAC: 08A:1E:B7:41:C6:23  Destination MAC: 001:00:5E:00:00:02
IP: 0845.177.065.242  IP: 224.0.0.0
Priority: 000  Priority: 000  State: 000  Hello: 003  Hold: 00A  Hold: 00FFF
Group: 000  Version: 080  Auth: cisco  VVIP: 0080.126.215.171
```

Figure III.27: Attaque HSRP

Résultat de l'attaque HSRP:



```
ESW1#
*Mar 1 00:55:12.055: %HSRP-5-STATECHANGE: Vlan10 Grp 10 state Active -> Speak
ESW1#
*Mar 1 00:55:22.055: %HSRP-5-STATECHANGE: Vlan10 Grp 10 state Speak -> Standby

ESW2#
*Mar 1 00:55:09.551: %HSRP-5-STATECHANGE: Vlan10 Grp 10 state Standby -> Listen
```

Figure III.28: Résultat de l'Attaque HSRP

**Critique et solution :**

D'après l'étude qu'on a fait et les tests de pénétration simulé on a déduit que le HSRP n'est pas fiable, parce que il n'aide pas à sécuriser notre topologie car les messages circule en claire, par contre le protocole de redondance GLPP est fiable et plus sécurisé, le trafic est bien crypté en plus il partage la charges entre les switches.



### **Conclusion**

Ce chapitre avait pour but de détailler les différentes phases d'implémentation de la solution proposée pour permettre interconnexion sécurisée de deux ou plusieurs sites distants tout en protégeant le Data Center de notre organisme d'accueil.

Ce chapitre avait également pour finalité de présenter toutes les configurations implémentées au niveau des équipements utilisés dans la nouvelle architecture réseau.

# Conclusion Général

## **Conclusion**

Le secteur des technologies de l'information étant en constante mutation, le présent travail fait état des résultats obtenus lors d'une simulation pour la mise en place d'un réseau VPN site to site. En effet, la mise en place de VPN site to site permet aux réseaux privés de s'étendre en étant séparés et reliés au moyen d'Internet.

Cette solution VPN au moyen du protocole IPSec apporte des bénéfices importants pour l'infrastructure réseau de notre entreprise, elle contribue à la réduction des coûts et participe également de façon considérable dans la sécurisation de notre infrastructure.

Notre travail fait pareillement état des résultats propres à la mise en place d'un serveur Radius, celui-ci étant connu Par sa capacité à centraliser les procédures d'admission d'un grand nombre d'utilisateurs, concourt la solution présentée ci-haut dans la sécurisation de notre infrastructure et ce, en agissant en tant qu'authentificateur des entités représentant l'organisme.

Le serveur Radius profite, quant à lui, de l'appui sécuritaire du serveur ISA qui fait l'objet de proxy filtrant les URLs auxquelles les utilisateurs essaient d'accéder et mettant en cache les pages web les plus consultées dans le but de réduire le temps d'accès à Internet.

Ces solutions, pour faire de notre organisation, une organisation sûre et non-sujette aux pannes et dont la disponibilité est assurée, sont déployées et secondés avec redondance étant faite par la réplique des équipements tels que les pare-feux et commutateurs, et réalisée au moyen des protocoles tels que FailOver, HSRP, EtherChannel et STP.

# Annexe

# Annexe

Annexe1: La configuration des routeurs R3 et FAI:

**R3 :**

**Les interfaces :**

```
!  
interface FastEthernet1/1  
no switchport  
ip address 60.60.60.2 255.255.255.0  
!  
interface FastEthernet1/2  
no switchport  
ip address 198.52.100.1 255.255.255.0  
!
```

**Routage :**

```
!  
ip route 0.0.0.0 0.0.0.0 60.60.60.1  
ip route 192.168.30.0 255.255.255.0 198.52.100.2  
ip route 198.51.100.0 255.255.255.0 60.60.60.1  
!
```

**Routeur FAI :**

**Les interfaces :**

```
!  
interface FastEthernet1/1  
no switchport  
ip address 198.51.100.101 255.255.255.0  
!  
interface FastEthernet1/2  
no switchport  
ip address 60.60.60.1 255.255.255.0  
!  
interface FastEthernet1/3  
no switchport  
ip address 50.50.50.1 255.255.255.0  
!
```

**Routeage :**

```
!  
ip route 192.168.11.0 255.255.255.0 198.51.100.100  
ip route 192.168.12.0 255.255.255.0 198.51.100.100  
ip route 192.168.30.0 255.255.255.0 198.52.100.2  
ip route 198.52.100.0 255.255.255.0 60.60.60.2  
!
```

## Annexe 2: configuration du firewall ASA3

### Les interfaces:

```
!
interface GigabitEthernet0
 nameif inside
 security-level 100
 ip address 192.168.12.1 255.255.255.0
!
interface GigabitEthernet1
 nameif DMZ
 security-level 50
 ip address 192.168.11.1 255.255.255.0
!
interface GigabitEthernet2
 nameif outside
 security-level 0
 ip address 198.51.100.100 255.255.255.0
!
interface GigabitEthernet3
 nameif management
 security-level 0
 ip address 192.168.40.254 255.255.255.0
!
```

### Routeage:

```
Gateway of last resort is 198.51.100.101 to network 0.0.0.0
C    192.168.12.0 255.255.255.0 is directly connected, inside
C    192.168.40.0 255.255.255.0 is directly connected, management
C    192.168.11.0 255.255.255.0 is directly connected, DMZ
C    198.51.100.0 255.255.255.0 is directly connected, outside
S*  0.0.0.0 0.0.0.0 [1/0] via 198.51.100.101, outside
```

### NAT:

```
object network LocalNetwork
 subnet 192.168.12.0 255.255.255.0
object network RemoteNetwork
 subnet 192.168.30.0 255.255.255.0
object network OutsideNetwork
 range 198.51.100.50 198.51.100.61
object network DMZSERVER
 host 192.168.11.3
object network OUTDMZ
 host 198.51.100.14
```

```
nat (inside,outside) source static LocalNetwork LocalNetwork destination static RemoteNetwork RemoteNetwork no
proxy-arp route-lookup
!
```

```
!
object network LocalNetwork
  nat (any,any) dynamic OutsideNetwork
object network DMZSERVER
  nat (DMZ,outside) static OUTDMZ
```

### VPN site to site:

```
crypto ikev1 enable outside
crypto ikev1 policy 1
  authentication pre-share
  encryption aes-256
  hash sha
  group 2
  lifetime 86400
```

```
access-list vpn-acl extended permit ip 192.168.12.0 255.255.255.0 192.168.1.0 255.255.255.0
```

```
crypto ipsec ikev1 transform-set ASA1Tranform-set esp-aes-256 esp-sha-hmac
crypto dynamic-map DYNMAP 65535 set ikev1 transform-set ASA1Tranform-set
crypto dynamic-map DYNMAP 65535 set reverse-route
crypto map ASA1VPN 1 match address Site1-to-Site2
crypto map ASA1VPN 1 set pfs
crypto map ASA1VPN 1 set peer 198.52.100.2
crypto map ASA1VPN 1 set ikev1 transform-set ASA1Tranform-set
crypto map ASA1VPN 1 set security-association lifetime seconds 28800
crypto map ASA1VPN 65535 ipsec-isakmp dynamic DYNMAP
crypto map ASA1VPN interface outside
crypto isakmp identity address
```

```
tunnel-group 198.52.100.2 type ipsec-l2l
tunnel-group 198.52.100.2 ipsec-attributes
  ikev1 pre-shared-key *****
```



## VPN Remote access:

```
username abdelmalek password /7n0qtk3B9eXX4Xk encrypted
```

```
group-policy GP internal
group-policy GP attributes
dns-server value 8.8.8.8
split-tunnel-policy tunnelspecified
split-tunnel-network-list value vpn-acl
```

```
tunnel-group TG type remote-access
tunnel-group TG general-attributes
address-pool VPNPOOL
default-group-policy GP
tunnel-group TG ipsec-attributes
ikev1 pre-shared-key *****
```

```
ip local pool VPNPOOL 192.168.1.10-192.168.1.15 mask 255.255.255.0
```

## ACL:

```
access-list Site1-to-Site2 extended permit ip object LocalNetwork object RemoteNetwork
access-list NAT extended permit ip object LocalNetwork object RemoteNetwork
access-list outside_access in extended permit tcp any object DMZSERVER eq www
access-list NAT_INSIDE extended permit ip host 192.168.12.5 host 50.50.50.2
access-list 101 extended permit icmp any any echo-reply
access-list 101 extended permit icmp any any echo
access-list 101 extended permit icmp any any source-quench
access-list 101 extended permit icmp any any unreachable
access-list 101 extended permit icmp any any time-exceeded
access-list 101 extended permit tcp any host 192.168.11.3 eq www
access-list vpn-acl extended permit ip 192.168.12.0 255.255.255.0 192.168.1.0 255.255.255.0
access-list 102 extended permit ip any any
```

```
access-group 101 in interface outside
```

## Annexe 3: configuration du firewall ASA4

### Les interfaces:

```
!
interface GigabitEthernet0
 nameif outside
 security-level 0
 ip address 198.52.100.2 255.255.255.0
!
interface GigabitEthernet1
 nameif inside
 security-level 100
 ip address 192.168.30.1 255.255.255.0
!
```

### NAT:

```
object network LocalNetwork
 subnet 192.168.30.0 255.255.255.0
object network OutsideNetwork
 range 198.52.100.50 198.52.100.61
object network RemoteNetwork
 subnet 192.168.12.0 255.255.255.0
```

```
object network LocalNetwork
 nat (any,any) dynamic OutsideNetwork
```

```
nat (inside,outside) source static LocalNetwork LocalNetwork destination static RemoteNetwork RemoteNetwork no-proxy-arp route-lookup
!
```

### Routage:

```
Gateway of last resort is 198.51.100.1 to network 0.0.0.0

C    192.168.30.0 255.255.255.0 is directly connected, inside
C    198.52.100.0 255.255.255.0 is directly connected, outside
S*  0.0.0.0 0.0.0.0 [1/0] via 198.51.100.1, outside
```

## VPN site to site:

```
crypto ipsec ikev1 transform-set ASA2Transform-set esp-aes-256 esp-sha-hmac
crypto map ASA2VPN 1 match address Site2-to-Site1
crypto map ASA2VPN 1 set pfs
crypto map ASA2VPN 1 set peer 198.51.100.100
crypto map ASA2VPN 1 set ikev1 transform-set ASA2Transform-set
crypto map ASA2VPN 1 set security-association-lifetime-seconds 28800
crypto map ASA2VPN interface outside
crypto isakmp identity address
crypto ikev1 enable outside
crypto ikev1 policy 1
```

```
authentication pre-share
encryption aes-256
hash sha
group 2
lifetime 86400
```

```
access-list Site2-to-Site1 extended permit ip object LocalNetwork object RemoteNetwork
access-list NAT extended permit ip object LocalNetwork object RemoteNetwork
```

```
tunnel-group 198.51.100.100 type ipsec-l2l
tunnel-group 198.51.100.100 ipsec-attributes
 ikev1 pre-shared-key *****
!
```

## Annexe 4: configuration des switches S1 et S2:

### Configuration du Switch S1:

#### Spanning tree:

```
spanning-tree vlan 10 priority 8192
spanning-tree vlan 20 priority 8192
```

#### Les interfaces et Etherchannel:

```
interface FastEthernet1/0
  switchport mode trunk
  duplex full
  speed 100
!
interface FastEthernet1/1
  switchport mode trunk
  duplex full
  speed 100
!
interface FastEthernet1/2
  switchport mode trunk
  duplex full
  speed 100
  channel-group 1 mode on
!
interface FastEthernet1/3
  switchport mode trunk
  duplex full
  speed 100
  channel-group 1 mode on
!
interface FastEthernet1/4
  switchport mode trunk
  duplex full
  speed 100
  channel-group 1 mode on
!
interface FastEthernet1/5
  switchport mode trunk
  duplex full
  speed 100
  channel-group 1 mode on
!
interface FastEthernet1/6
  no switchport
  ip address 172.16.1.3 255.255.255.0
  duplex full
  speed 100
!
```

## VLAN et GLBP:

```
interface Vlan10
 ip address 192.168.10.1 255.255.255.0
 glbp 1 ip 192.168.10.50
 glbp 1 priority 150
 glbp 1 preempt
!
interface Vlan20
 ip address 192.168.20.1 255.255.255.0
 glbp 1 ip 192.168.20.50
 glbp 1 priority 150
 glbp 1 preempt
!
```

## Routage:

```
router eigrp 20
 network 172.16.1.0 0.0.0.255
 network 192.168.10.0
 network 192.168.20.0
 no auto-summary
!
```

## Configuration du Switch S2:

### Spanning Tree:

```
!
spanning-tree vlan 10 priority 8191
spanning-tree vlan 20 priority 8191
```

## Les interfaces et Etherchannel:

```
!  
interface FastEthernet1/0  
  switchport mode trunk  
  duplex full  
  speed 100  
!  
interface FastEthernet1/1  
  switchport mode trunk  
  duplex full  
  speed 100  
!  
interface FastEthernet1/2  
  switchport mode trunk  
  duplex full  
  speed 100  
  channel-group 1 mode on  
!  
interface FastEthernet1/3  
  switchport mode trunk  
  duplex full  
  speed 100  
  channel-group 1 mode on  
!  
interface FastEthernet1/4  
  switchport mode trunk  
  duplex full  
  speed 100  
  channel-group 1 mode on  
!  
interface FastEthernet1/5  
  switchport mode trunk  
  duplex full  
  speed 100  
  channel-group 1 mode on  
!  
interface FastEthernet1/6  
  no switchport  
  ip address 172.16.1.4 255.255.255.0  
  duplex full  
  speed 100  
!
```

## Routage:

```
!  
router eigrp 20  
network 172.16.1.0 0.0.0.255  
network 192.168.10.0  
network 192.168.20.0  
no auto-summary  
!  
!
```

## VLAN et GLBP:

```
!  
interface Vlan10  
ip address 192.168.10.2 255.255.255.0  
glbp 1 ip 192.168.10.50  
glbp 1 priority 120  
glbp 1 preempt  
!  
interface Vlan20  
ip address 192.168.20.2 255.255.255.0  
glbp 1 ip 192.168.20.50  
glbp 1 priority 120  
glbp 1 preempt  
!
```

## Annexe 5: configuration des firewalls ASA 1 et ASA 2:

### Configuration du firewall ASA1:

#### Configuration des interface et failover:

```
interface GigabitEthernet0
 nameif inside
 security-level 100
 ip address 172.16.1.1 255.255.255.0 standby 172.16.1.2
!
interface GigabitEthernet1
 description LAN Failover Interface
!
interface GigabitEthernet2
 nameif outside
 security-level 0
 ip address 172.16.2.1 255.255.255.0 standby 172.16.2.2
!
```

```
failover
failover lan unit primary
failover lan interface FO GigabitEthernet1
failover key *****
failover interface ip FO 10.1.0.1 255.255.255.0 standby 10.1.0.2
```

#### ACL:

```
access-list 102 extended permit icmp any any source-quench
access-list 102 extended permit icmp any any unreachable
access-list 102 extended permit icmp any any time-exceeded
access-list 102 extended permit tcp any host 192.168.10.20 eq ftp
access-list 102 extended permit tcp any host 192.168.10.20 eq 14147
access-list 102 extended permit tcp any host 192.168.10.20 eq ftp-data
access-list 102 extended permit tcp any host 192.168.10.20 gt 1024
access-list 102 extended permit tcp any host 192.168.20.20 eq www
access-list 102 extended permit tcp any host 192.168.20.20 eq https
access-list 102 extended permit udp any host 192.168.10.21 eq bootpc
access-list 102 extended permit udp any host 192.168.10.21 eq bootps
```



```
access-group 102 in interface outside
!
```

## Routage:

```
router eigrp 20
no auto-summary
network 172.16.1.0 255.255.255.0
network 172.16.2.0 255.255.255.0
!
```

## Configuration du firewall ASA2:

### interface et Failover:

```
interface GigabitEthernet0
nameif inside
security-level 100
ip address 172.16.1.1 255.255.255.0 standby 172.16.1.2
!
interface GigabitEthernet1
description LAN Failover Interface
!
interface GigabitEthernet2
nameif outside
security-level 0
ip address 172.16.2.1 255.255.255.0 standby 172.16.2.2
!
```

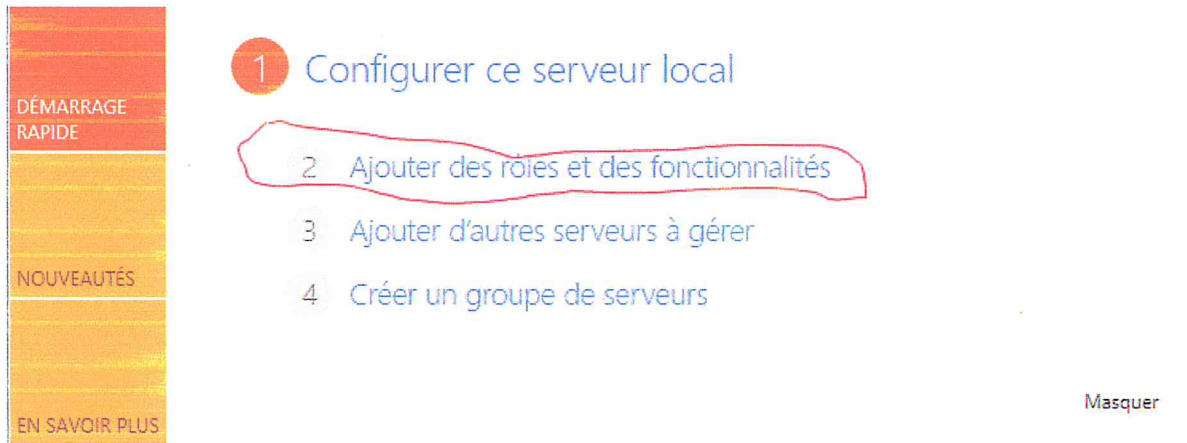
```
failover
failover lan unit secondary
failover lan interface FO GigabitEthernet1
failover key *****
failover interface ip FO 10.1.0.1 255.255.255.0 standby 10.1.0.2
```

## ANNEXE 6

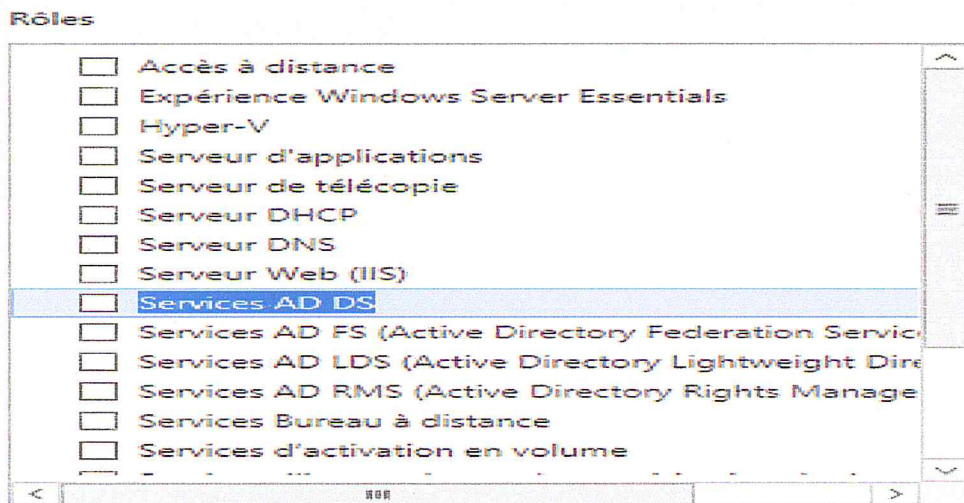
### INSTALLATION DE L'ACTIVE DIRECTORY SUR WINDOWS (SERVER 2012 R2)

- Installation du rôle « Contrôleur du domaine Active Directory »

Pour ajouter un rôle, un simple clique sur **Ajouter des rôles** :



Sélectionner le rôle « **Services de domaine Active Directory** ». L'assistant suit son cours et termine sur un rapport d'installation.



Avant de commencer  
Type d'installation  
Sélection du serveur  
Rôles de serveurs  
Fonctionnalités  
AD DS  
**Confirmation**  
Résultats

Pour installer les rôles, services de rôle ou fonctionnalités suivants sur le serveur sélectionné, cliquez sur Installer.

Redémarrer automatiquement le serveur de destination, si nécessaire

Il se peut que des fonctionnalités facultatives (comme des outils d'administration) soient affichées sur cette page, car elles ont été sélectionnées automatiquement. Si vous ne voulez pas installer ces fonctionnalités facultatives, cliquez sur Précédent pour désactiver leurs cases à cocher.

Gestion de stratégie de groupe  
Outils d'administration de serveur distant  
Outils d'administration de rôles  
Outils AD DS et AD LDS  
Module Active Directory pour Windows PowerShell  
Outils AD DS  
Centre d'administration Active Directory  
Composants logiciels enfichables et outils en ligne de commande AD DS  
Services AD DS

[Exporter les paramètres de configuration](#)  
[Spécifier un autre chemin d'accès source](#)

< Précédent

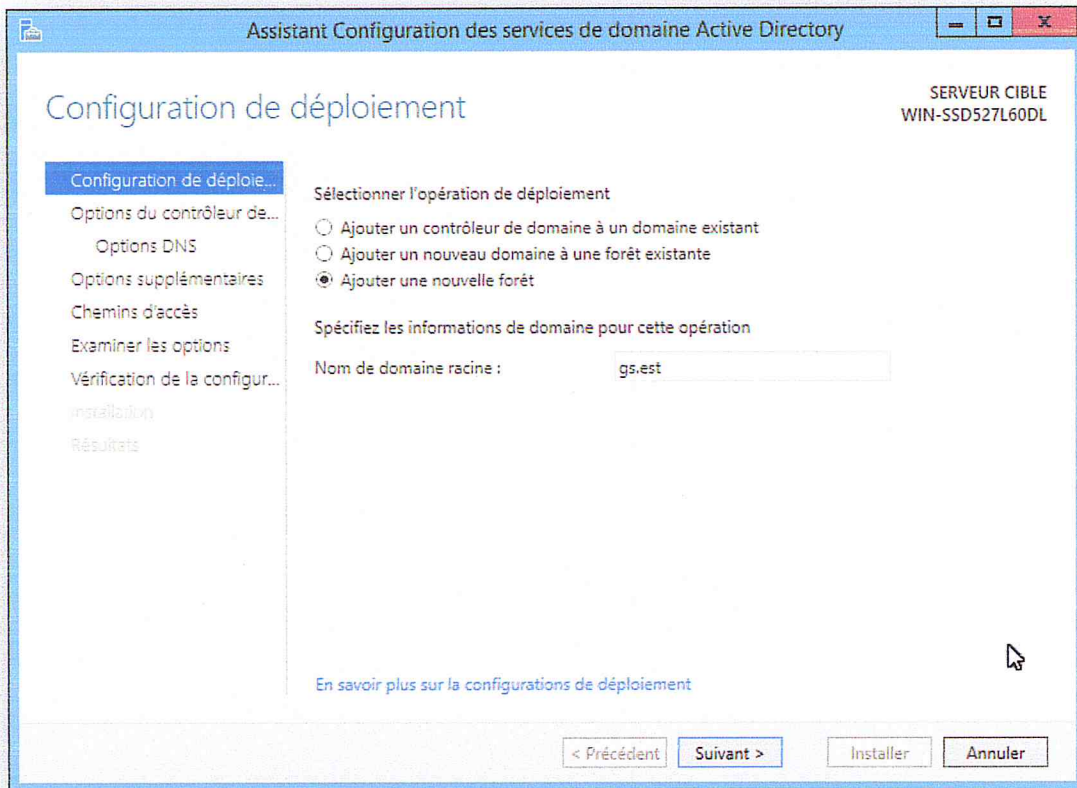
Suivant >

Installer

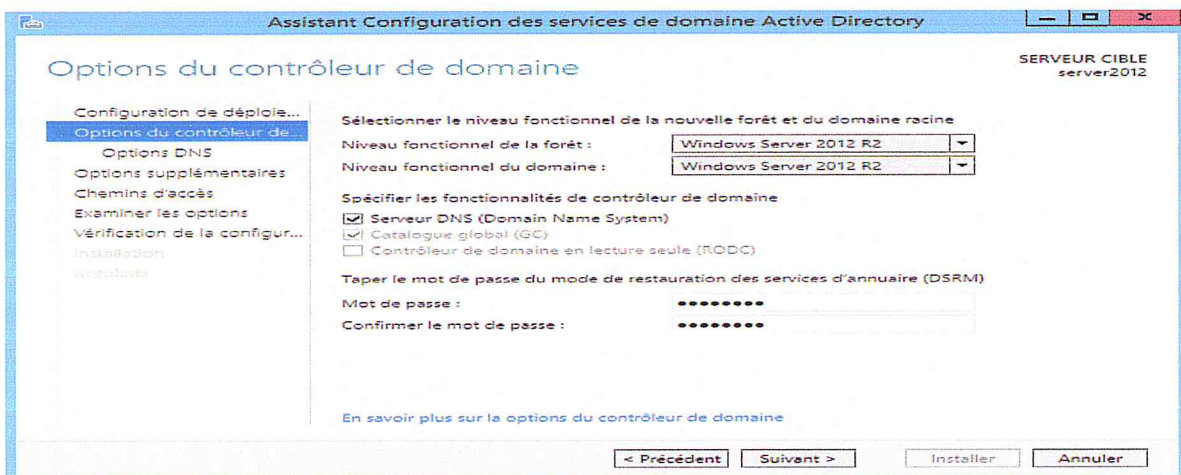
Annuler

Explorateur de fichiers

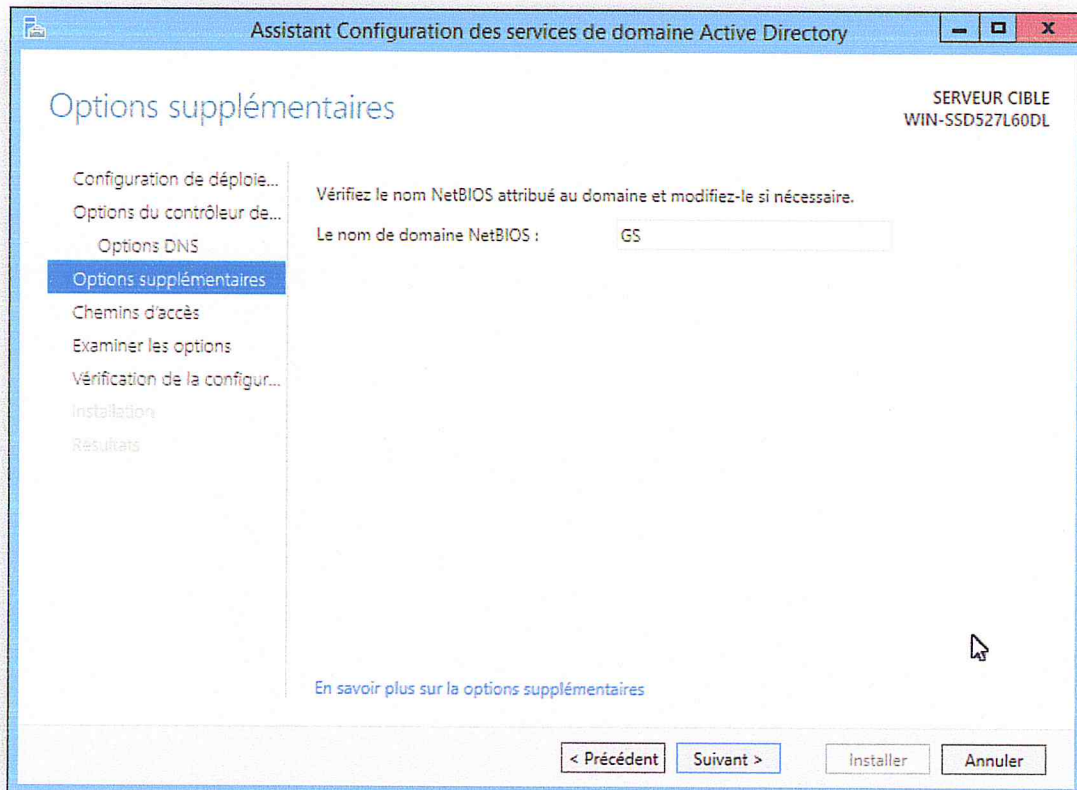
Après l'installation du rôle Active directory par le biais de l'assistant d'installation, on passe à Active Directory Domain Services Configuration Wizard et Sélectionner l'option « **Créer un domaine dans une nouvelle forêt** » ensuite Saisir le nom du domaine **gs.est** et cliquer sur Suivant :



Définir un mot de passe de restauration. Ce mot de passe sera indispensable pour réaliser des opérations de maintenance sur la base de données

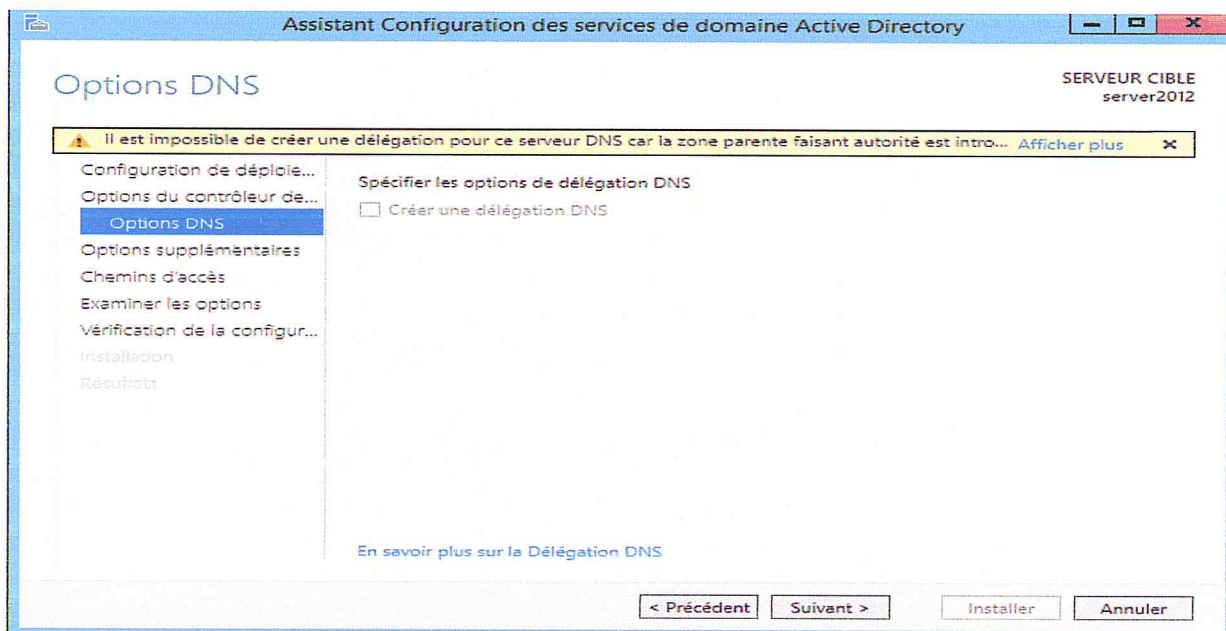


Ensuite, nous allons désigner le nom **NetBIOS**, qui est une réminiscence des anciens systèmes Windows et encore utilisé par de nombreux éditeurs de logiciels. Il est préférable de le laisser tel que l'assistant le génère : **GS**

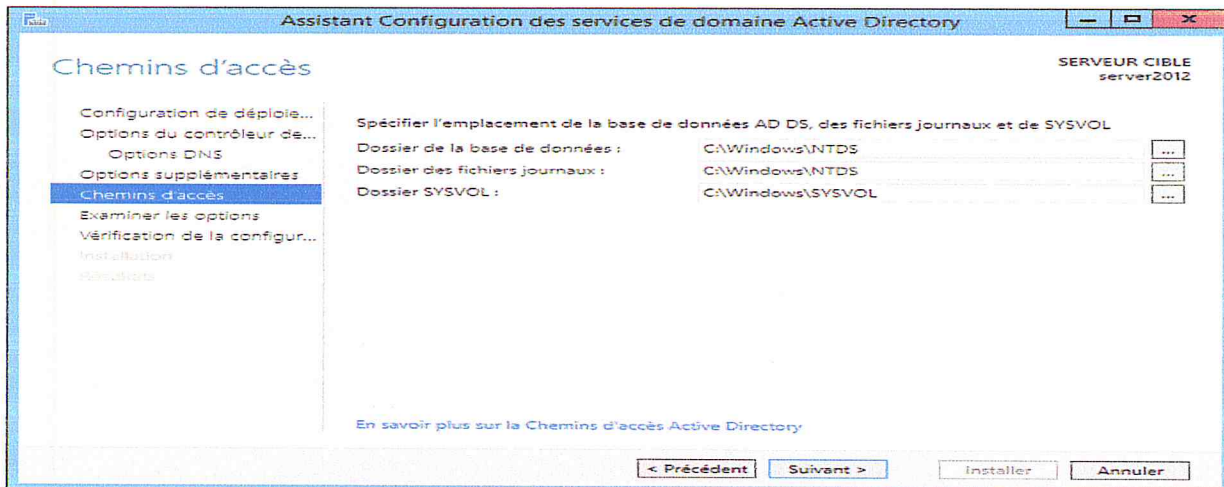


Le DNS sera installé en même temps que l'Active Directory

Cliquez sur oui pour installer le service de domaine Active Directory



Placer, de préférence, la base NTDS dans un emplacement sécurisé

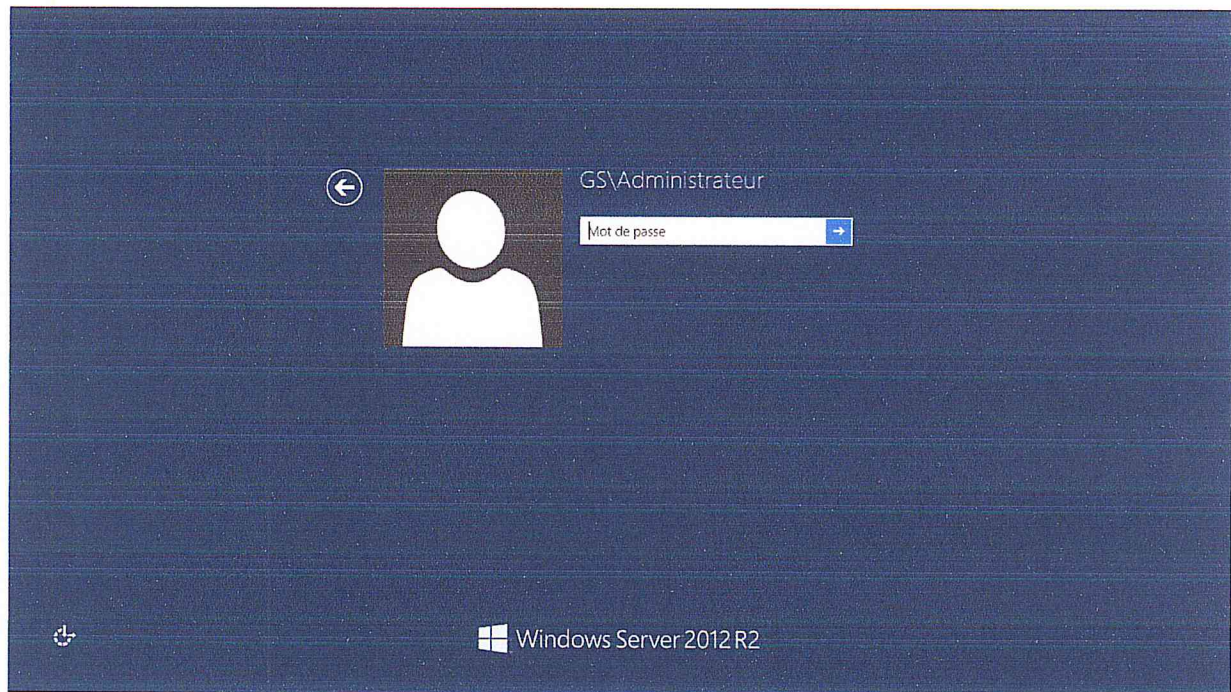


Cochez le bouton radio "**Redémarrer à la fin de l'opération**", pour la prise en charge des nouveaux paramètres de configuration après le redémarrage du serveur.

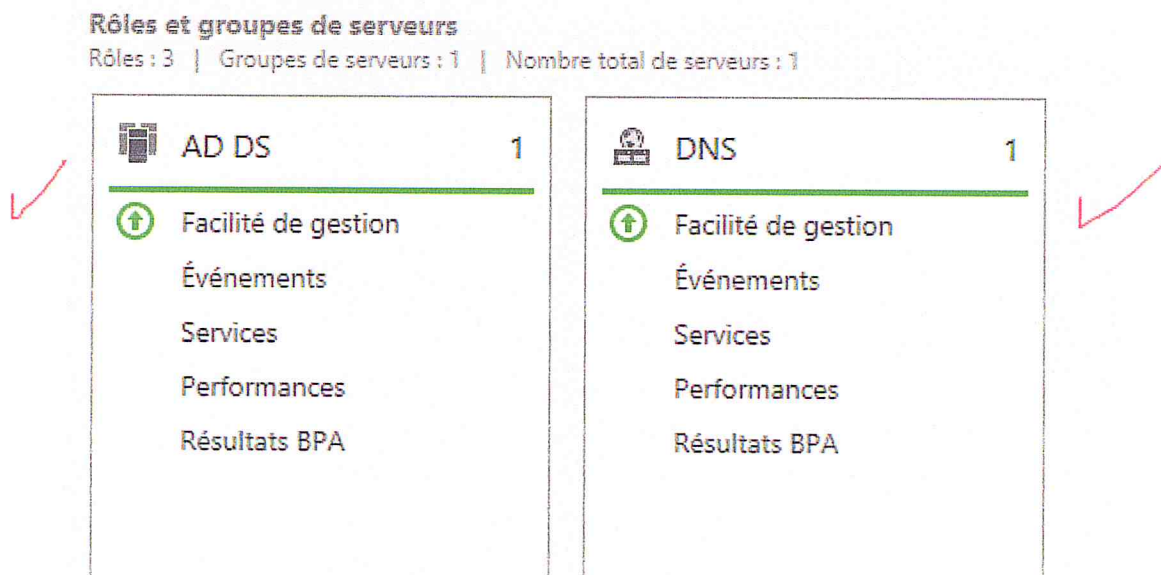
Lors du redémarrage vous pouvez constater que la mire de connexion est changée puisque l'authentification s'effectue désormais sur le domaine GS.

Vous devez utiliser le premier mot de

Passer du compte **pc** utilisé auparavant



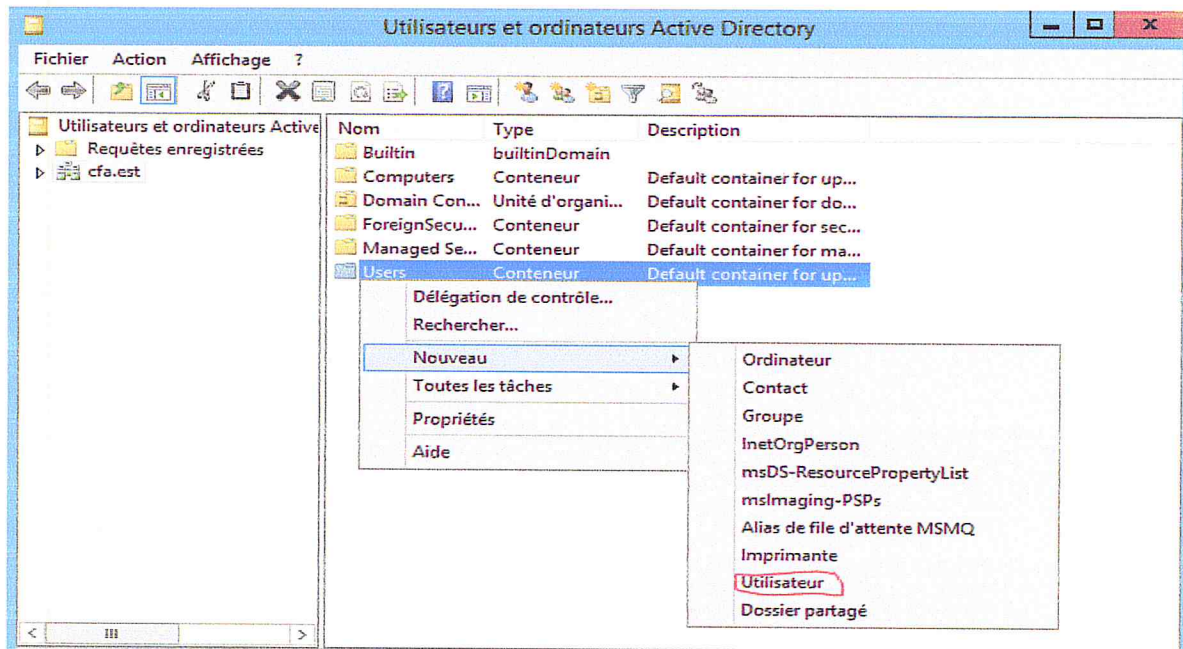
Une fois le redémarrage automatique effectué, l'Active Directory est installé et opérationnel. Pour Vérifier l'installation correcte du Rôle DNS, aller dans à la fenêtre "**Gestionnaire de serveur**" vous observez que le rôle "**DNS**" et le rôle "**Service de domaine Active Directory**" ont bien été installés.



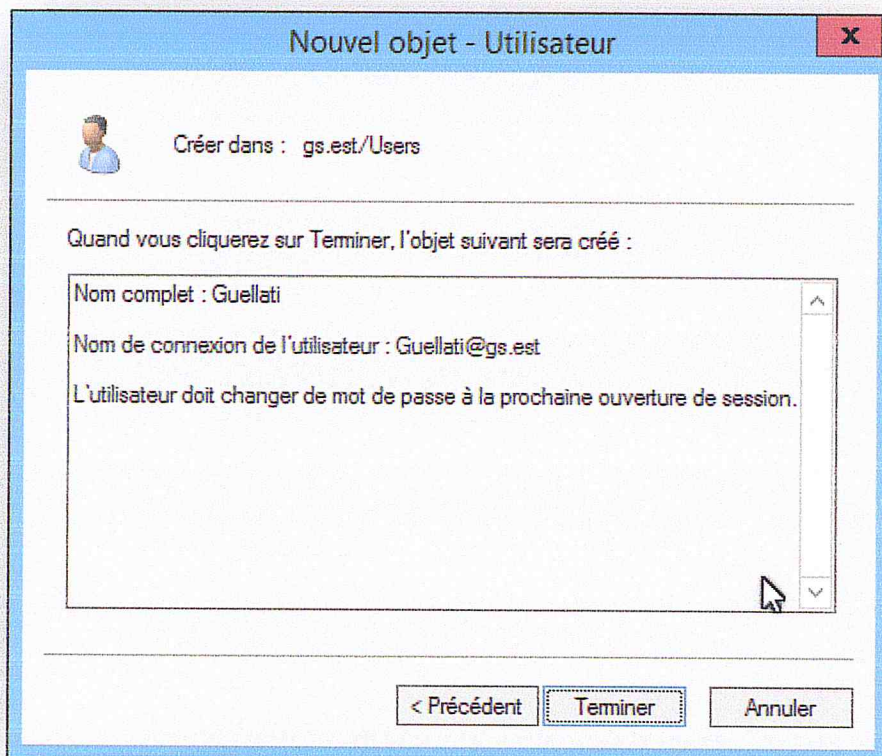
- **Ajout d'un utilisateur au domaine**

Pour créer un nouvel utilisateur, développez le rôle "**Service de domaine Active Directory**", aller dans le dossier "**Users**", clique droit, "**Nouveau**" puis "**Utilisateur**".



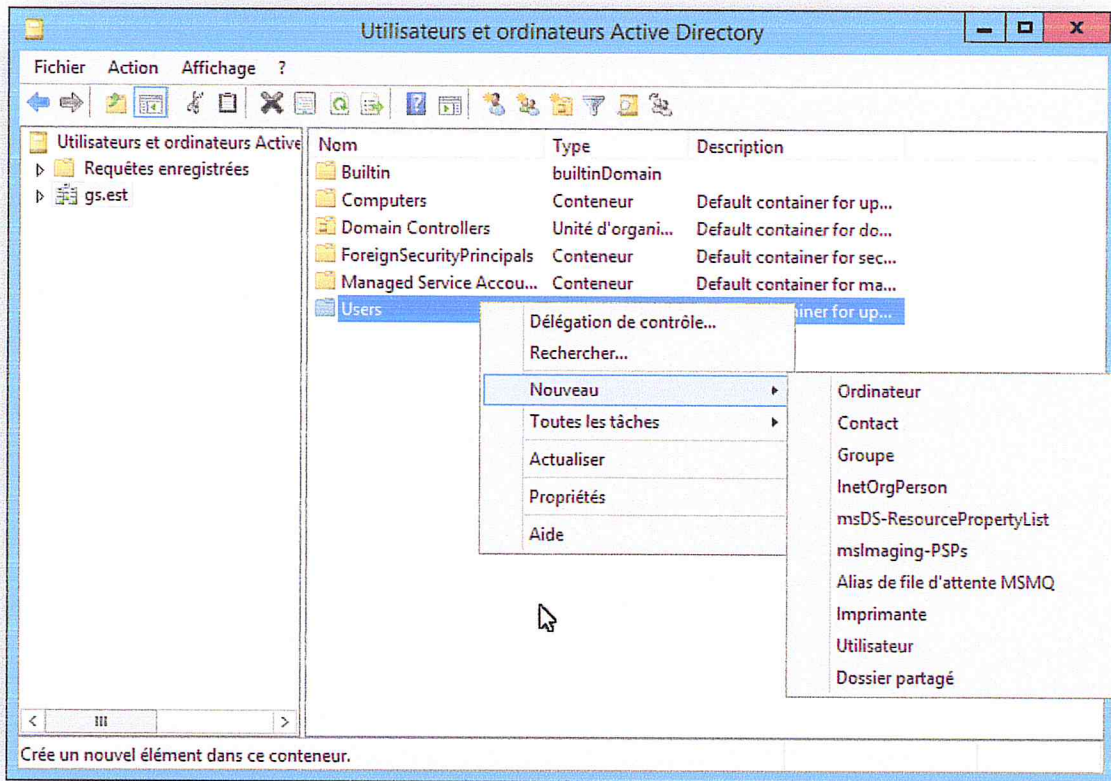


Remplir les différents champs et entrer un mot de passe, puis choisir une stratégie du compte, ensuite cliquez sur "**Terminez**", ainsi, le premier utilisateur a été ajouté.

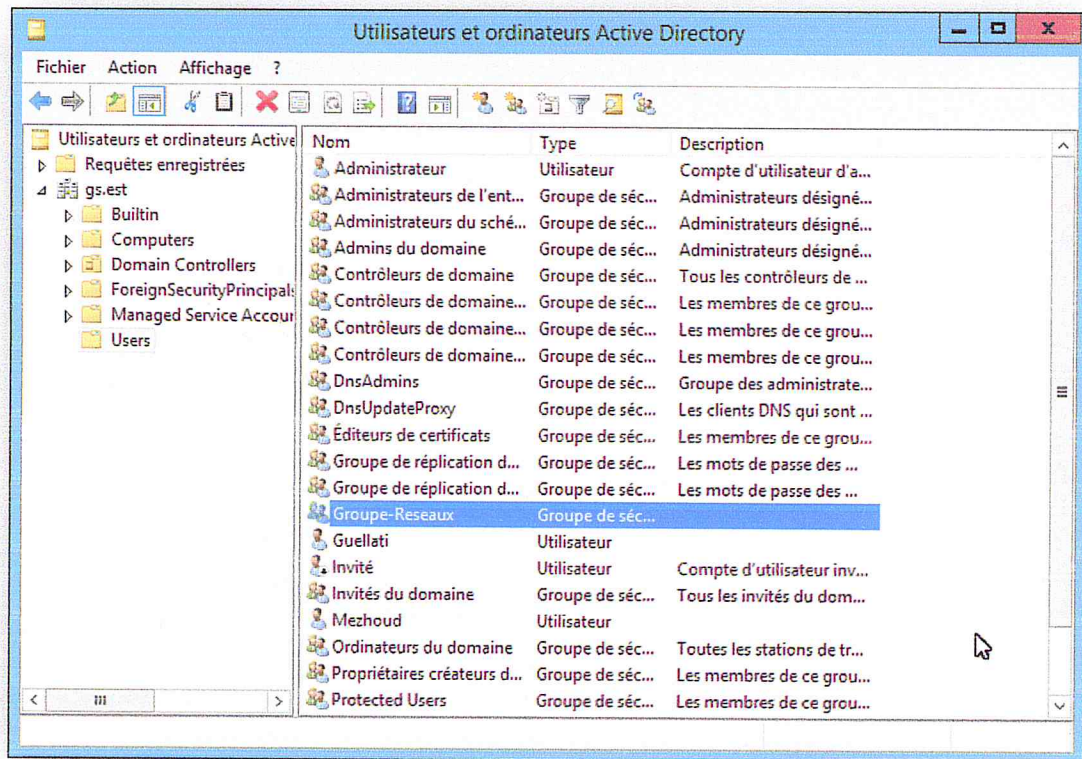


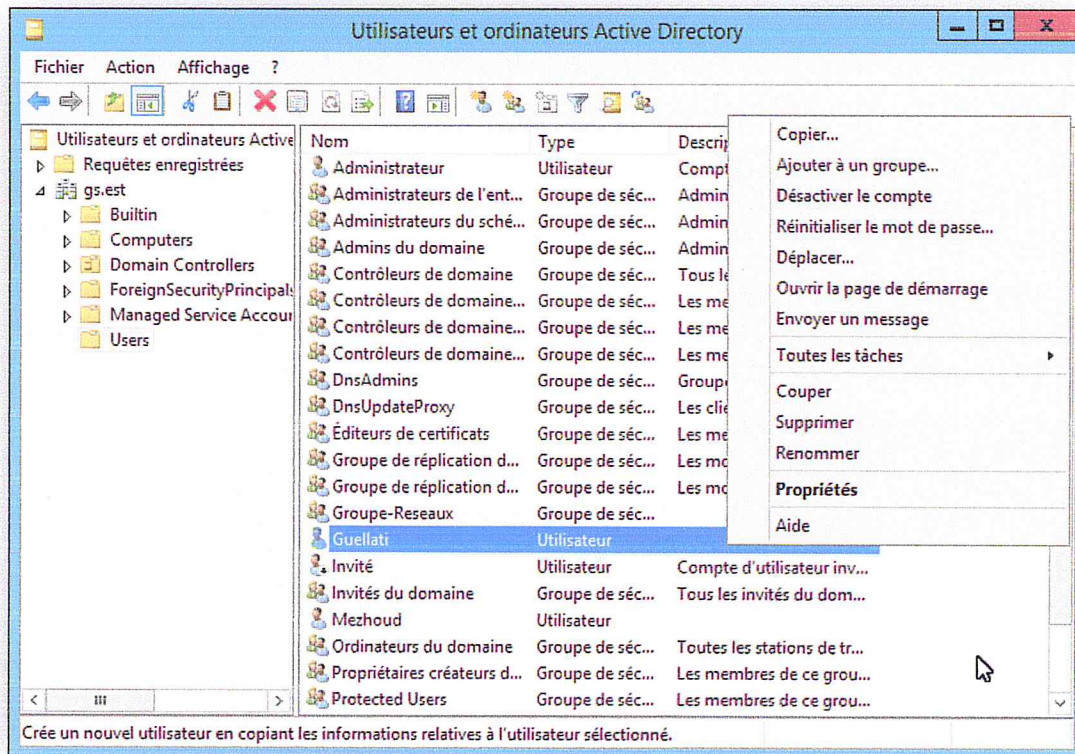
- **Ajout d'un groupe au domaine**

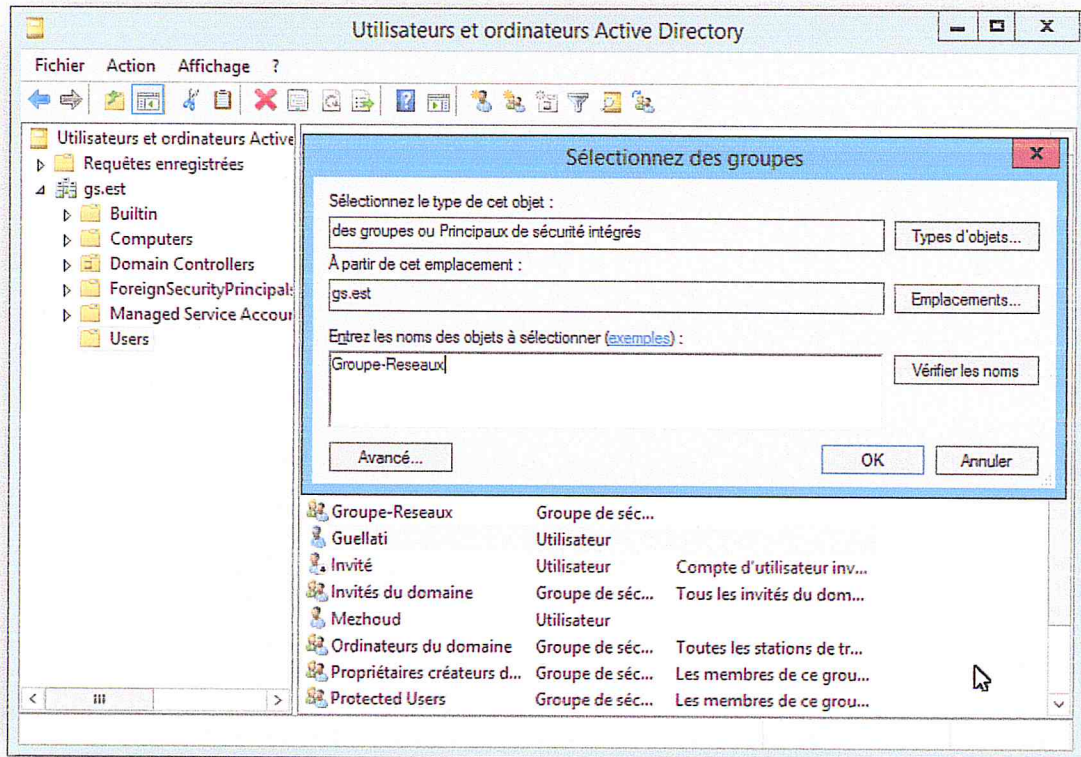
Pour créer un nouveau groupe, développez le rôle "Service de domaine Active Directory», aller dans le dossier "Users", clique droit, "Nouveau" puis "Groupe".

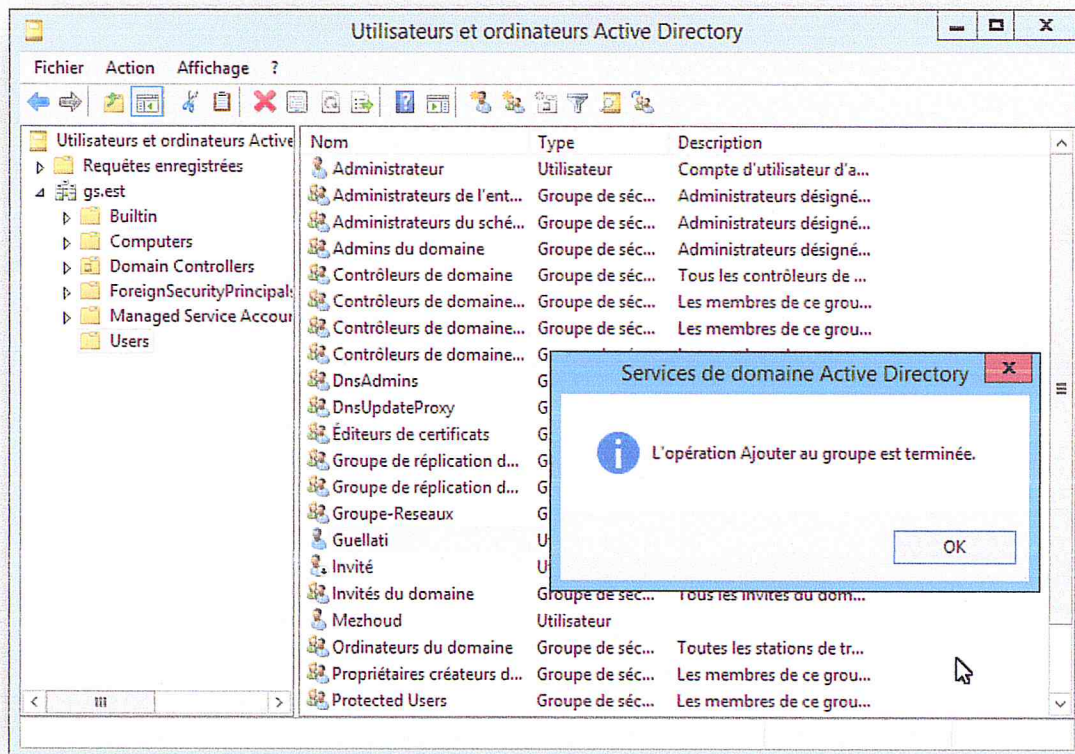


Pour ajouter un utilisateur au groupe, on clique sur ajouter, puis on sélectionne l'utilisateur dans l'annuaire :





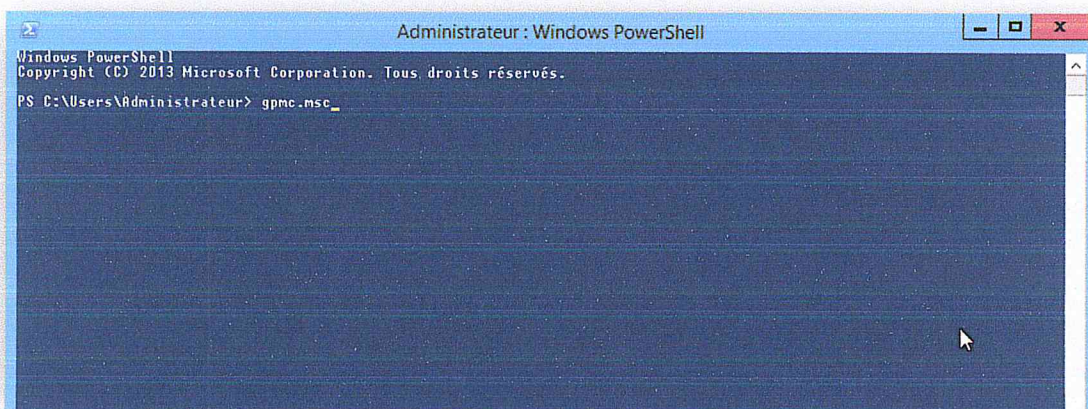




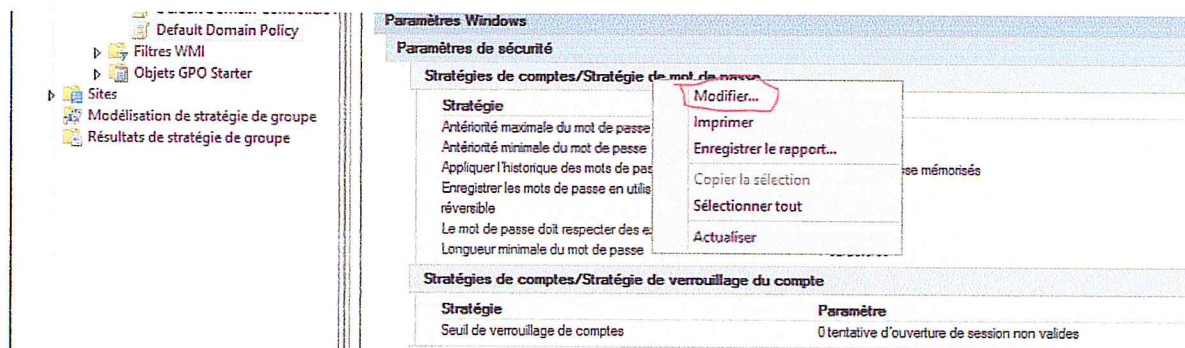
- **Modification de la stratégie de groupe**

La stratégie de groupe est l'outil standard pour gérer, de façon centralisée, les règles qui doivent contrôler les utilisateurs en matière de gestion **de mot de passe** par exemple qui vont permettre d'exiger certaines limitations lors de la définition des mots de passe. Pour modifier la stratégie du groupe on va suivre les étapes suivantes:

Démarrage de la console «gestion des stratégies de groupe» en utilisant la commande «**gpmc.msc**» :



Cliquer sur le bouton droit sur **Stratégie de comptes/Stratégie de mot de passe** puis sélectionné « **modifier**»



La **Stratégie de mot de passe** va nous permettre d'exiger certains paramètres de stratégie à respecter lors de la définition des mots de passe des utilisateurs, à savoir :

- **Conserver l'historique des mots de passe** : Cette stratégie permet aux administrateurs d'améliorer la sécurité en garantissant que d'anciens mots de passe ne sont pas réutilisés continuellement en déterminant le nombre de nouveaux mots de passe uniques devant être associés à un compte d'utilisateur avant qu'un ancien mot de passe puisse être réutilisé.
- **Durée de vie maximale du mot de passe** : Détermine la période (en jours) pendant laquelle un mot de passe peut être utilisé avant que le système oblige l'utilisateur à le changer.
- **Durée de vie minimale du mot de passe** : Détermine la période minimale (en jours) d'utilisation d'un mot de passe avant que l'utilisateur puisse le changer.

**Enregistrer le mot de passe en utilisant un cryptage réversible** : détermine si le système d'exploitation enregistre les mots de passe en utilisant un chiffrement réversible. Cette stratégie est requise lors de l'utilisation de l'authentification CHAP par accès distant ou IAS. Elle est aussi requise lors de l'utilisation de l'authentification Digest dans IIS.

- **Le mot de passe doit respecter des exigences de complexité** : Détermine si les mots de passe doivent respecter des exigences de complexité. Les mots de passe doivent respecter les exigences minimales suivantes :
  - Ne pas contenir le nom de compte de l'utilisateur ou des parties du nom complet de l'utilisateur comptant plus de deux caractères successifs.
  - Comporter au moins six caractères.
  - Contenir des caractères provenant de trois des quatre catégories suivantes :
    - Caractères majuscules anglais (A à Z).
    - Caractères minuscules anglais (a à z).

- Chiffres en base 10 (0 à 9).
- Caractères non alphabétiques (par exemple, \*, !, \$, #, %).

**Longueur minimale du mot de passe :** Détermine le nombre minimal de caractères que doit contenir le mot de passe d'un compte d'utilisateur.

Ensuit :

1. Sélectionnez l'interface réseau ou les interfaces réseau.
2. Entrez ensuite le nom du domaine, l'adresse IP du serveur DNS local, puis l'adresse IP du serveur DNS public.
3. Configurer ensuite les étendues d'adresse IP qui seront distribuées par le serveur. Cliquez sur « **Ajouter** ».
4. Lorsque vous avez ajouté les étendues souhaitées, cliquez sur « **Suivant** ».
5. L'assistant d'installation vous demande si vous voulez configurer le serveur en IPv6. N'ayant que des adresses IPv4, on sélectionne la deuxième option (**Disable DHCPv6**).

On vous demande ensuite le login de l'administrateur autorisé à ajouter un serveur dans le domaine. (Ce message s'affiche si le serveur est intégré au domaine).

- **Intégrer une machine dans le domaine AD**

Afin d'intégrer un nouveau poste de travail dans le domaine AD, il est nécessaire de suivre les étapes suivante :

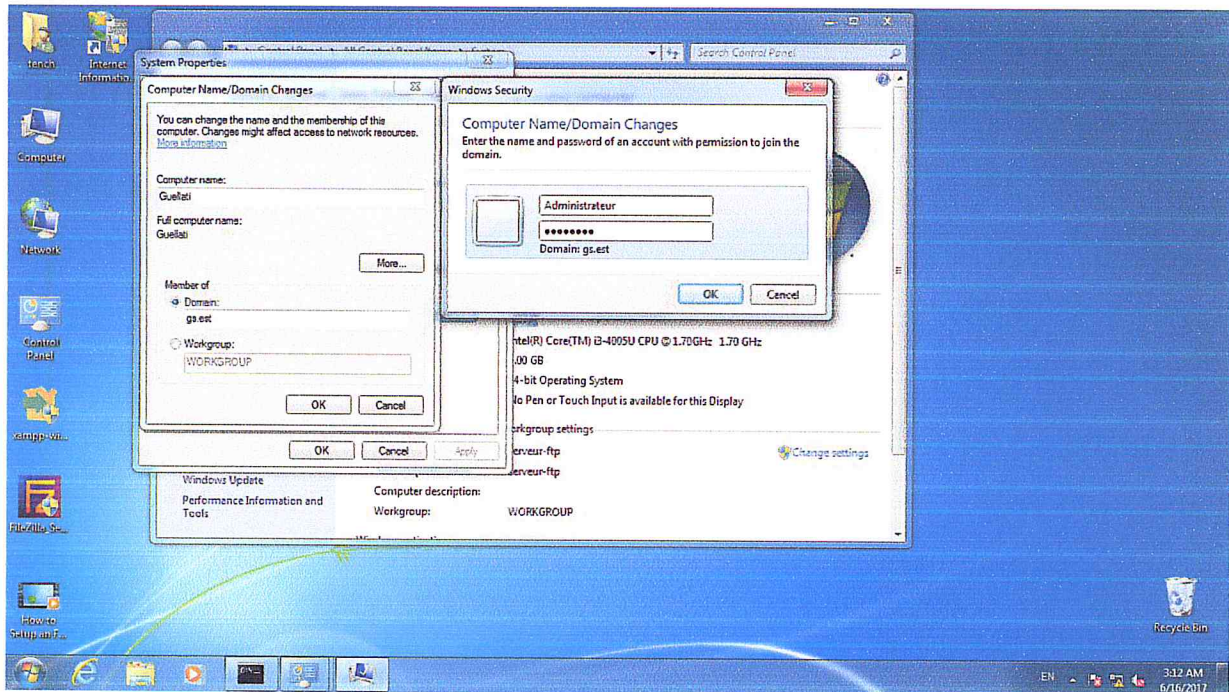
- Sélectionner l'adresse IP, le masque sous réseau

Ainsi que l'adresse IP du DNS automatiquement .

- Modification du nom de la machine et redémarrage

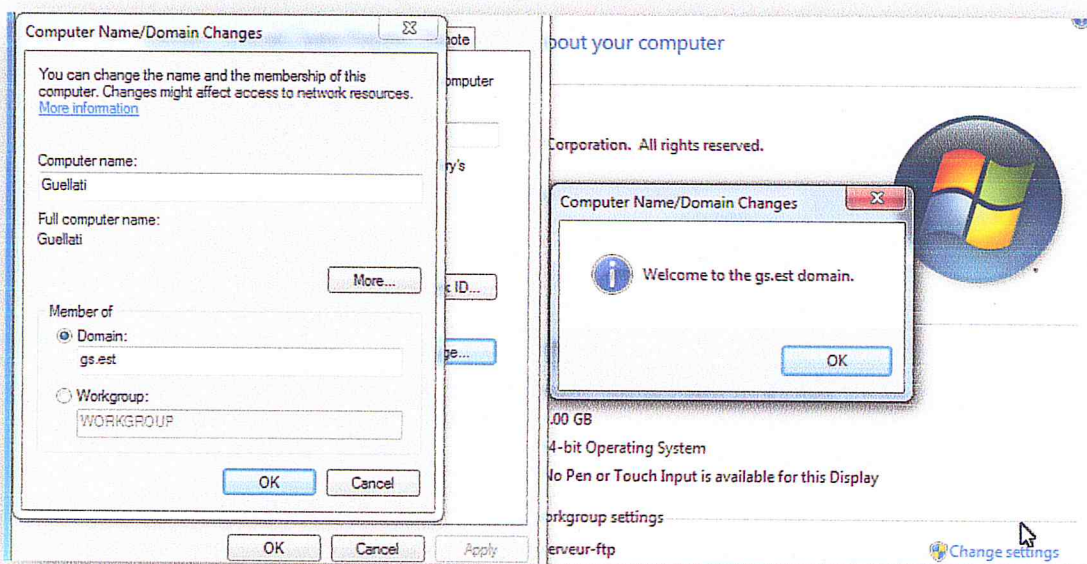
de la machine.



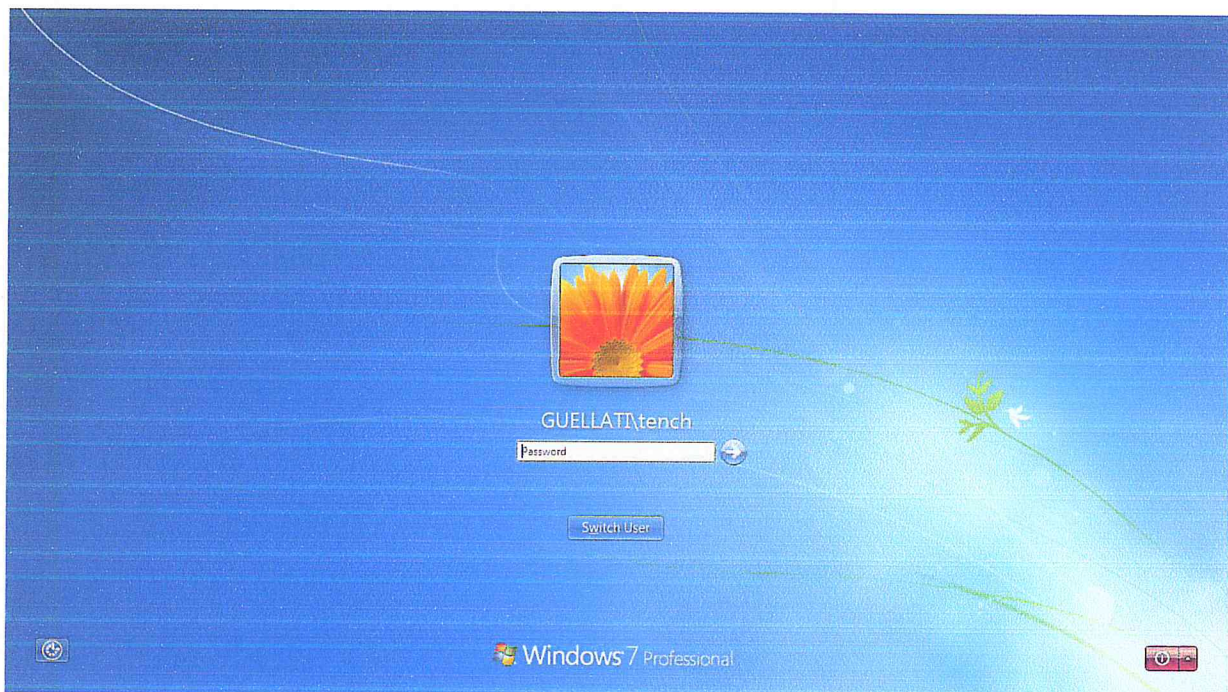
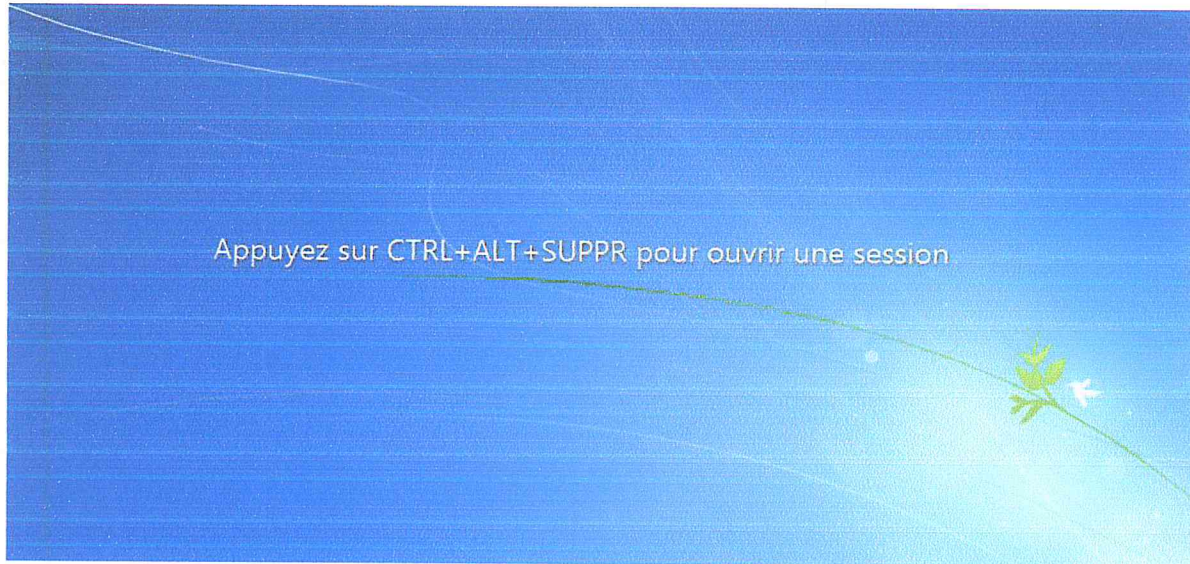


- Station de travail vous demande alors le nom d'utilisateur et le mot de passe d'un compte qui autorise l'intégration de la machine au domaine (administrateur de domaine).

- Confirmation de l'intégration de la machine dans le domaine et invite pour le redémarrage de la machine.



Après le redémarrage vous obtenez l'écran en face Sélectionner "**Ctrl + Alt + Suppr**" et entrer le nom d'utilisateur sur le domaine, le mot de passe associé puis on clique sur "Options" pour sélectionner le domaine au quel on veut se connecter via le menu déroulant.



- **Groupes de sécurité**

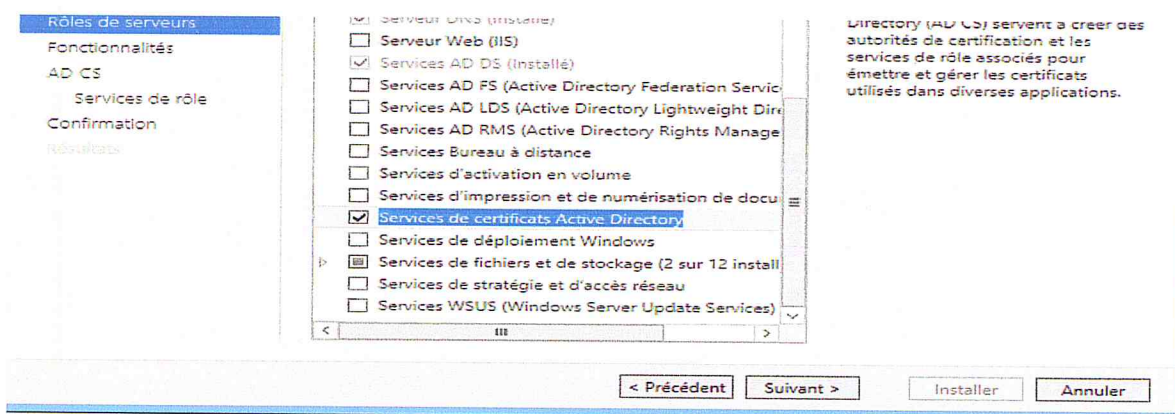
Pour que notre NPS puisse authentifier nos différents *Supplicants*, il faut lui fournir un groupe de sécurité dans lequel il va contrôler l'identité du *Supplicant*, nous avons donc créé des groupes .

## INSTALLATION DU ROLE SERVICES DE CERTIFICAT AD

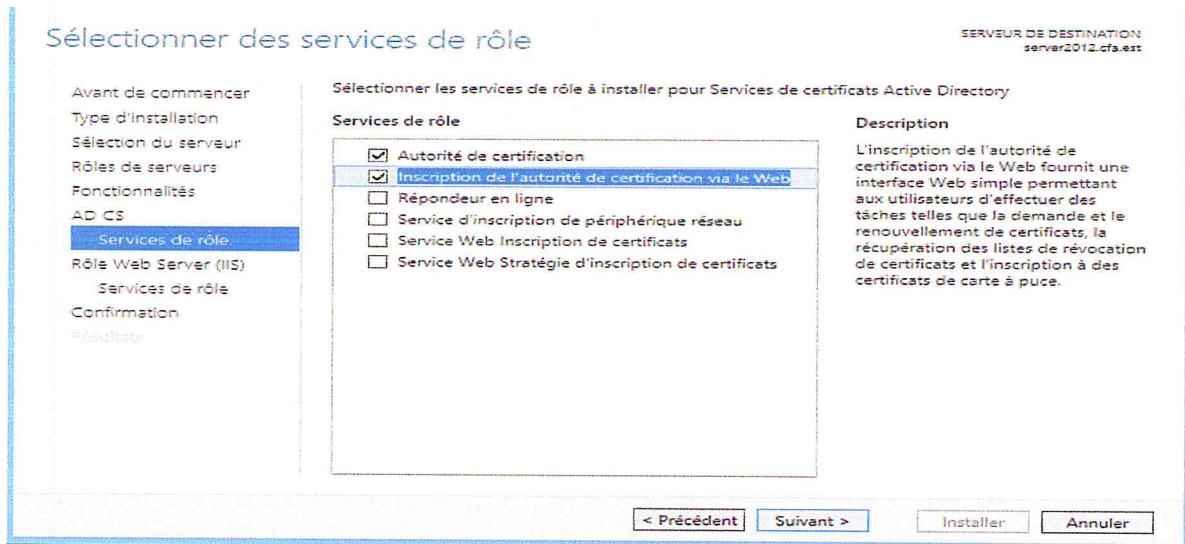
Dans cette annexe, nous allons présenter les différentes étapes nécessaires pour la mise en place d'une plate-forme de gestion de clé **PKI**, ceci va nous permettre de générer des certificats conformes à la norme **x509**, pour les différents clients afin de renforcer le processus d'authentification.

- **Procédure d'installation du rôle AD CS**

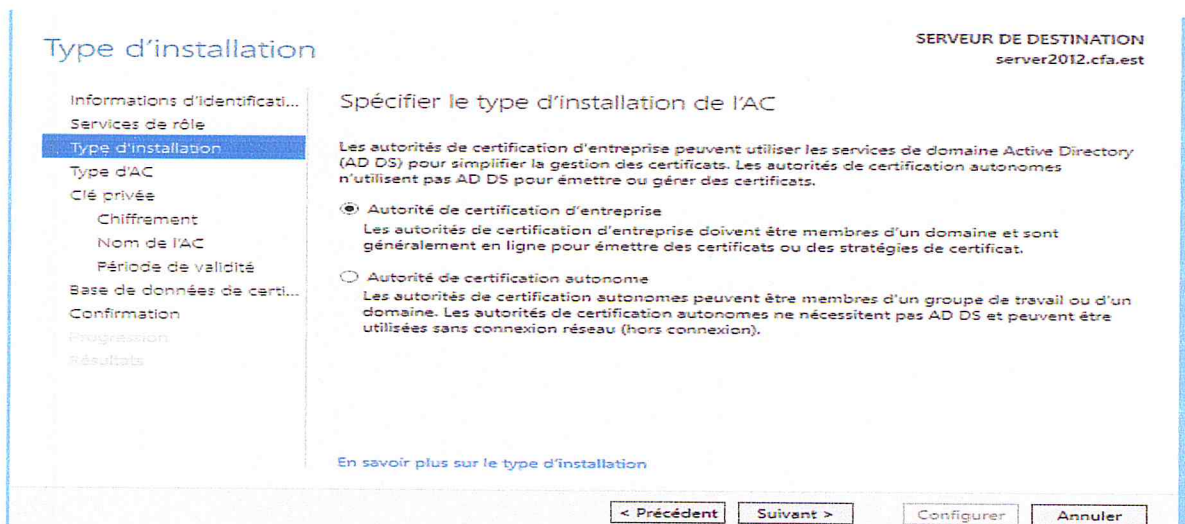
1. Dans le gestionnaire du serveur on clique sur « **Ajouter des rôles** » puis on sélectionne « **Service de certificats Active Directory** »



Sélection de « **autorité de certification** », et « **inscription de l'autorité de certification via le web** »



1. Sélection du type d'installation « **Entreprise** » pour pouvoir Utiliser les données d'Active Directory ainsi que pour Simplifier l'émission et la gestion des certificats puis cliquer sur suivant :



Sélection de **autorité de certification racine** » puis cliquer sur suivant :

## Type d'autorité de certification

SERVEUR DE DESTINATION  
server2012.cfa.est

- Informations d'identificati...
- Services de rôle
- Type d'installation
- Type d'AC
- Clé privée
- Chiffrement
- Nom de l'AC
- Période de validité
- Base de données de certifi...
- Confirmation
- Progression
- Résultats

### Spécifier le type de l'AC

Lorsque vous installez les services de certificats Active Directory (AD CS), vous créez ou étendez une hiérarchie d'infrastructure à clé publique (PKI). Une autorité de certification racine se trouve au sommet de la hiérarchie PKI et émet ses propres certificats auto-signés. Une autorité de certification secondaire reçoit un certificat de l'autorité de certification de rang plus élevé dans la hiérarchie PKI.

- Autorité de certification racine  
Les autorités de certification racines sont les premières voire les seules autorités de certification configurées dans une hiérarchie PKI.
- Autorité de certification secondaire  
Les autorités de certification secondaires nécessitent une hiérarchie PKI établie et sont autorisées à émettre des certificats par l'autorité de certification de rang plus élevé dans la hiérarchie.

[En savoir plus sur le type d'autorité de certification](#)

< Précédent

Suivant >

Configurer

Annuler

Créé une nouvelle clé privée puis cliquer sur suivant :

## Clé privée

SERVEUR DE DESTINATION  
server2012.cfa.est

- Informations d'identificati...
- Services de rôle
- Type d'installation
- Type d'AC
- Clé privée
- Chiffrement
- Nom de l'AC
- Période de validité
- Base de données de certifi...
- Confirmation
- Progression
- Résultats

### Spécifier le type de la clé privée

Pour générer et émettre des certificats aux clients, une autorité de certification doit posséder une clé privée.

- Créer une clé privée  
Utilisez cette option si vous n'avez pas de clé privée ou pour en créer une.
- Utiliser la clé privée existante  
Utilisez cette option pour garantir la continuité avec les certificats émis antérieurement lors de la réinstallation d'une AC.
  - Sélectionner un certificat et utiliser sa clé privée associée  
Sélectionnez cette option s'il existe un certificat sur cet ordinateur ou pour importer un certificat et utiliser sa clé privée associée.
  - Sélectionner une clé privée existante sur cet ordinateur  
Sélectionnez cette option si vous avez conservé les clés privées d'une installation antérieure ou pour utiliser une clé privée d'une autre source.

[En savoir plus sur la clé privée](#)

< Précédent

Suivant >

Configurer

Annuler

L'étape suivante consiste au choix de la méthode de chiffrement, dans notre cas on qui est le **SHA1** avec une taille de clé de **2048** :

## Chiffrement pour l'autorité de certification

SERVEUR DE DESTINATION  
server2012.cfa.est

Informations d'identificati...  
Services de rôle  
Type d'installation  
Type d'AC  
Clé privée  
**Chiffrement**  
Nom de l'AC  
Période de validité  
Base de données de certifi...  
Confirmation  
Progression  
Résultats

### Spécifier les options de chiffrement

Sélectionnez un fournisseur de chiffrement : RSA#Microsoft Software Key Storage Provider Longueur de la clé : 2048

Sélectionnez l'algorithme de hachage pour signer les certificats émis par cette AC :

- SHA256
- SHA384
- SHA512
- SHA1

Autorisez l'interaction de l'administrateur lorsque l'autorité de certification accède à la clé privée.

[En savoir plus sur le chiffrement](#)

< Précédent Suivant > Configurer Annuler

Pour terminer, il faut fixer la durée de validité des certificats générés par cette autorité. Ensuite, spécifier l'emplacement de la base de données des certificats.

Période de validité

server2012.cfa.est

Informations d'identificati...  
Services de rôle  
Type d'installation  
Type d'AC  
Clé privée  
Chiffrement  
Nom de l'AC  
**Période de validité**  
Base de données de certifi...  
Confirmation  
Progression  
Résultats

### Spécifier la période de validité

Sélectionnez la période de validité du certificat généré pour cette autorité de certification :

20 Années

Date d'expiration de l'AC : 21/04/2038 21:00:00

La période de validité configurée pour ce certificat d'autorité de certification doit dépasser la période de validité pour les certificats qu'elle émettra.

[En savoir plus sur la période de validité](#)

< Précédent Suivant > Configurer Annuler

Base de données de l'autorité de certification

SERVEUR DE DESTINATION  
server2012.cfa.est

Informations d'identificati...  
Services de rôle  
Type d'installation  
Type d'AC  
Clé privée  
Chiffrement  
Nom de l'AC  
Période de validité  
**Base de données de certifi...**  
Confirmation  
Progression  
Résultats

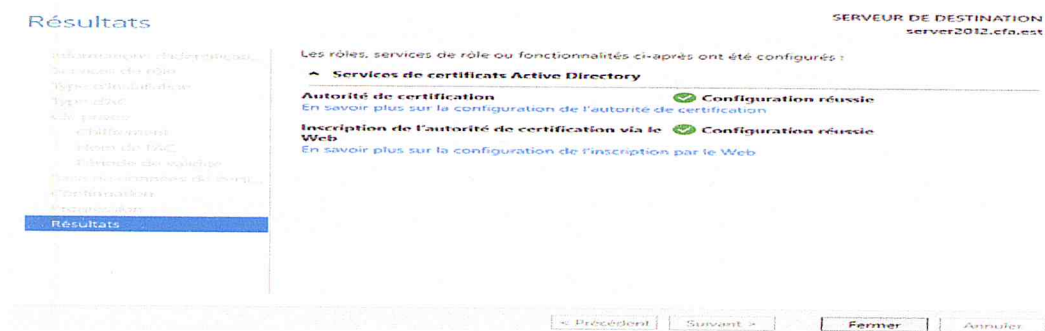
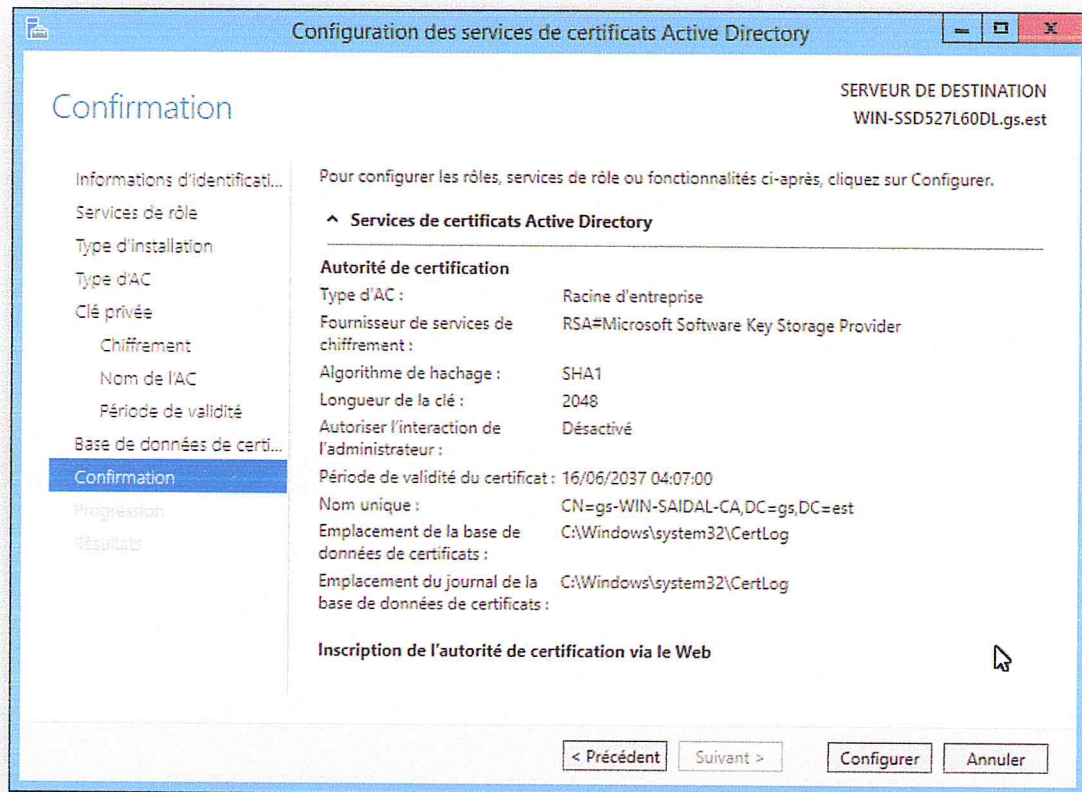
### Spécifier les emplacements des bases de données

Emplacement de la base de données de certificats : C:\Windows\system32\Certlog

Emplacement du journal de la base de données de certificats : C:\Windows\system32\Certlog

[En savoir plus sur la base de données de l'autorité de certification](#)

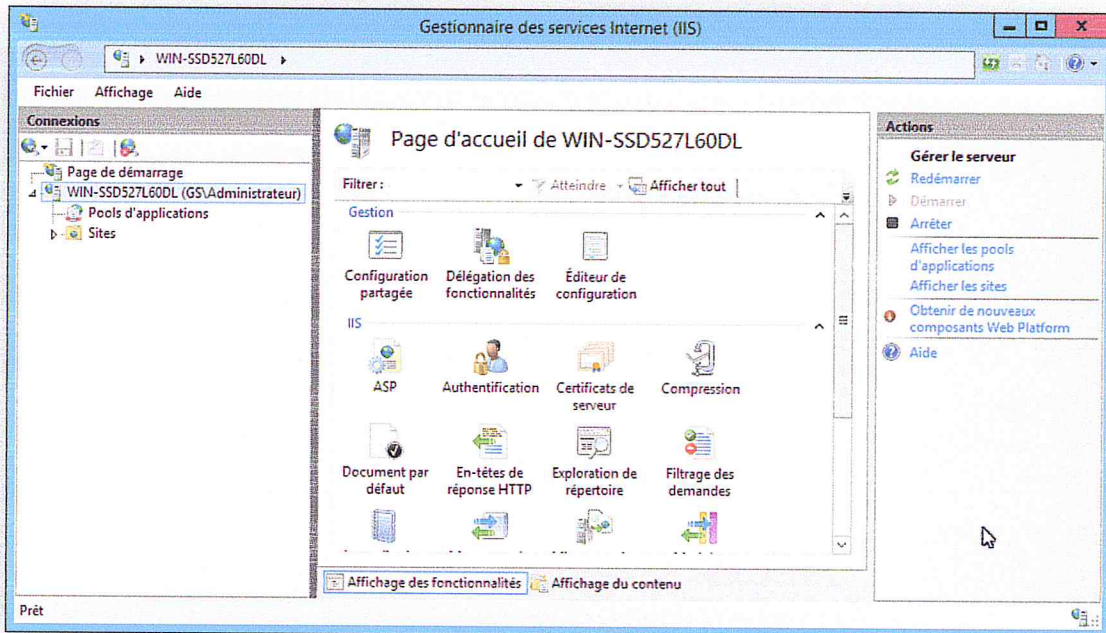
< Précédent Suivant > Configurer Annuler



- ❖ **Note** : La distribution des certificats se fera soit par une clé USB ou via le web. Concernant le deuxième cas, il faut installer un serveur web IIS.

- **Sécurisation du site pour l'échange des certificats**

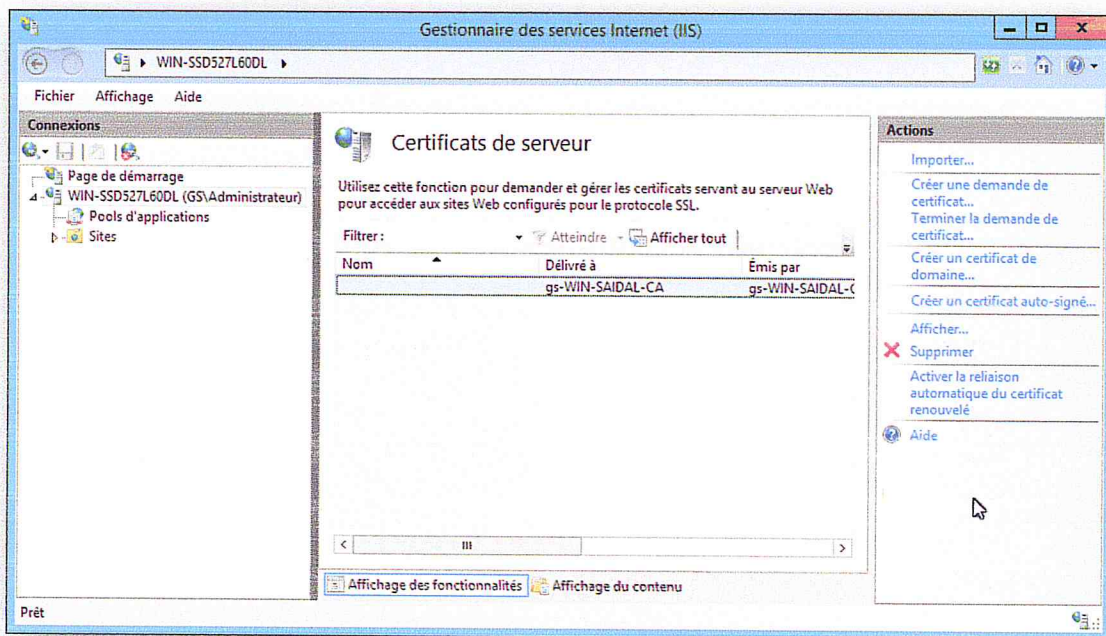
Donc une fois l'autorité de Certification installée, on va créer un certificat SSL pour le serveur afin de pouvoir demander un certificat, car par défaut on ne peut pas demander un certificat en utilisant http (sécurité requise). Pour cela on se connecte sur la console **mme** Gestionnaire de services internet.



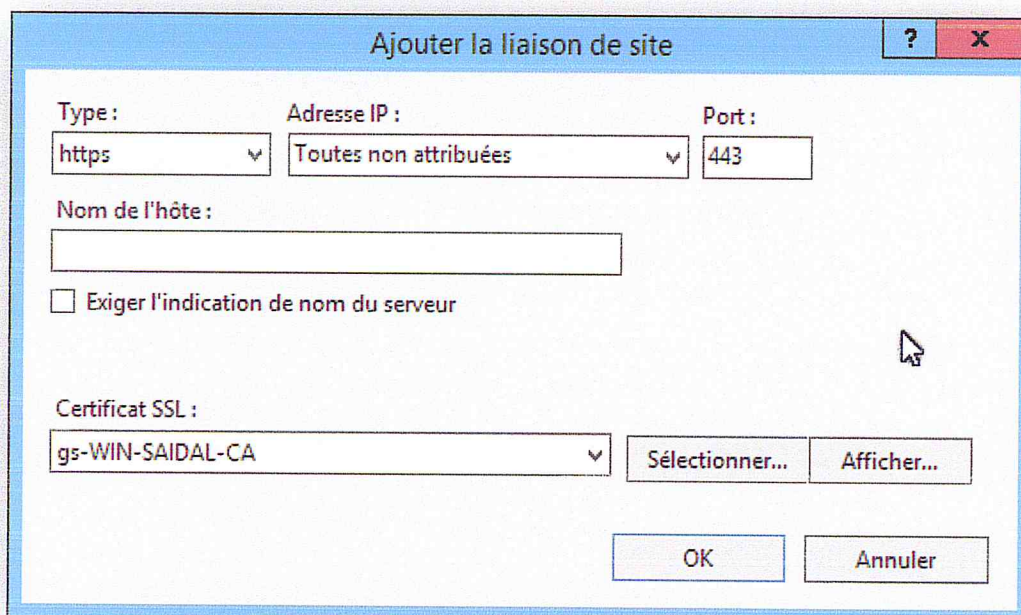
- **Création d'un certificat auto-signé**

Pour créer un certificat auto-signé il faut sélectionner « **Créer un certificat auto-signé** » dans le volet « **Actions** »

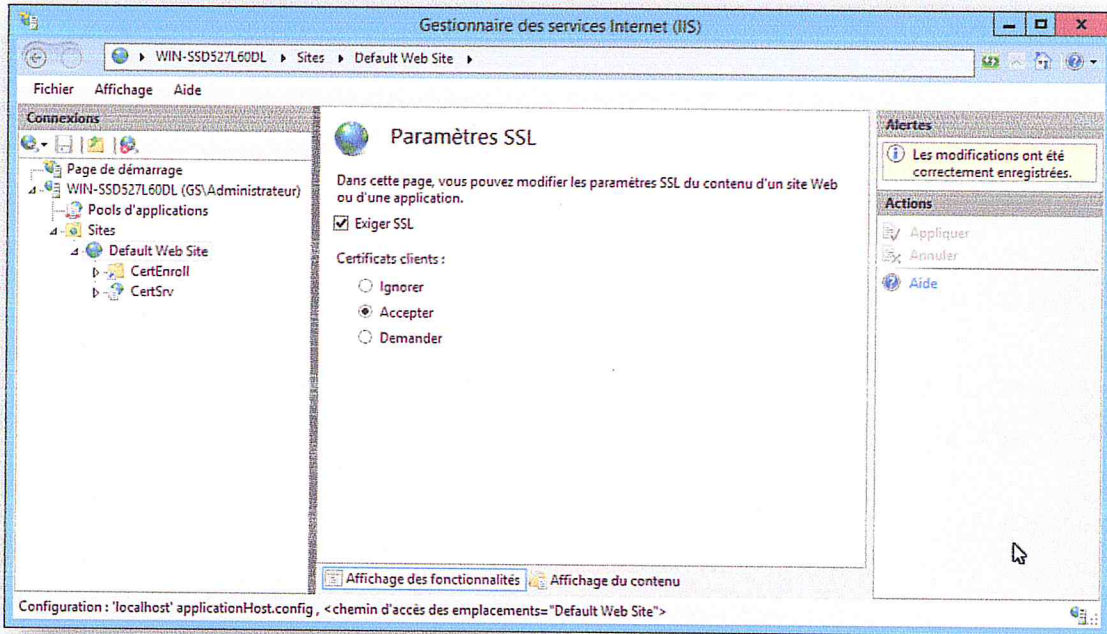




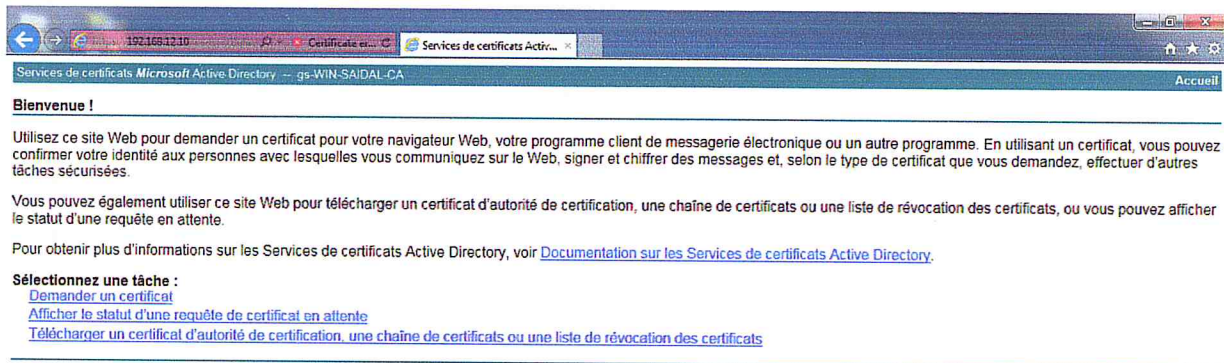
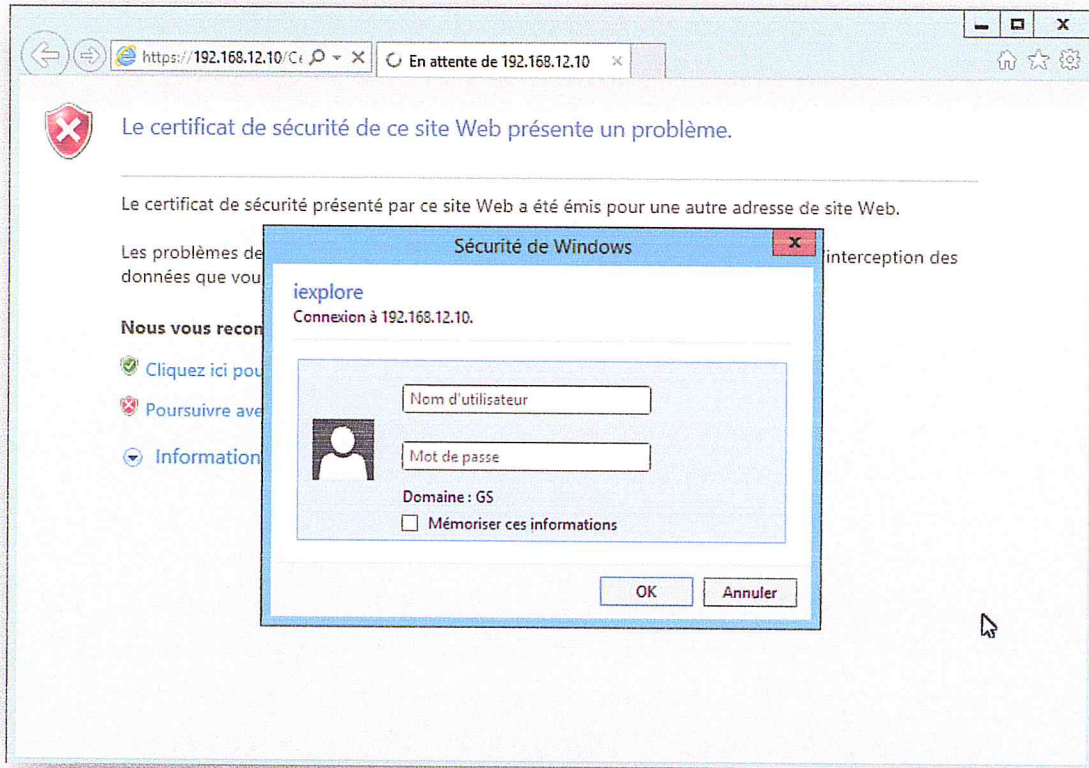
Maintenant que le certificat est créé, on va configurer notre site web (**certsrv**) en utilisant le port **443**, on va ajouter une liaison **https** sur le site de demande de certificat, en cliquant sur le bouton puis sur « **modifier les liaisons** » et enfin on clique sur « **ajouter** », là il faut choisir **https** et ensuite le certificat que nous venons de créer et en termine par validation.



Pour forcer l'accès web en SSL au niveau de IIS, on sélectionne le site « **certsrv** » et on clique sur « **paramètres SSL** » en cochant « **Exige SSL** »



A ce stade, l'autorité de certification est déployée et nous pouvons demander des certificats directement sur l'interface WEB: <https://radius:443/CertSrv> ou l'adresse du serveur



- **Demander et installer des certificats utilisateur :**

Pour autoriser les connexions des différents utilisateurs du domaine, il faut installer un certificat serveur pour chaque utilisateur.

Le procédé d'installation du certificat est comme suit :

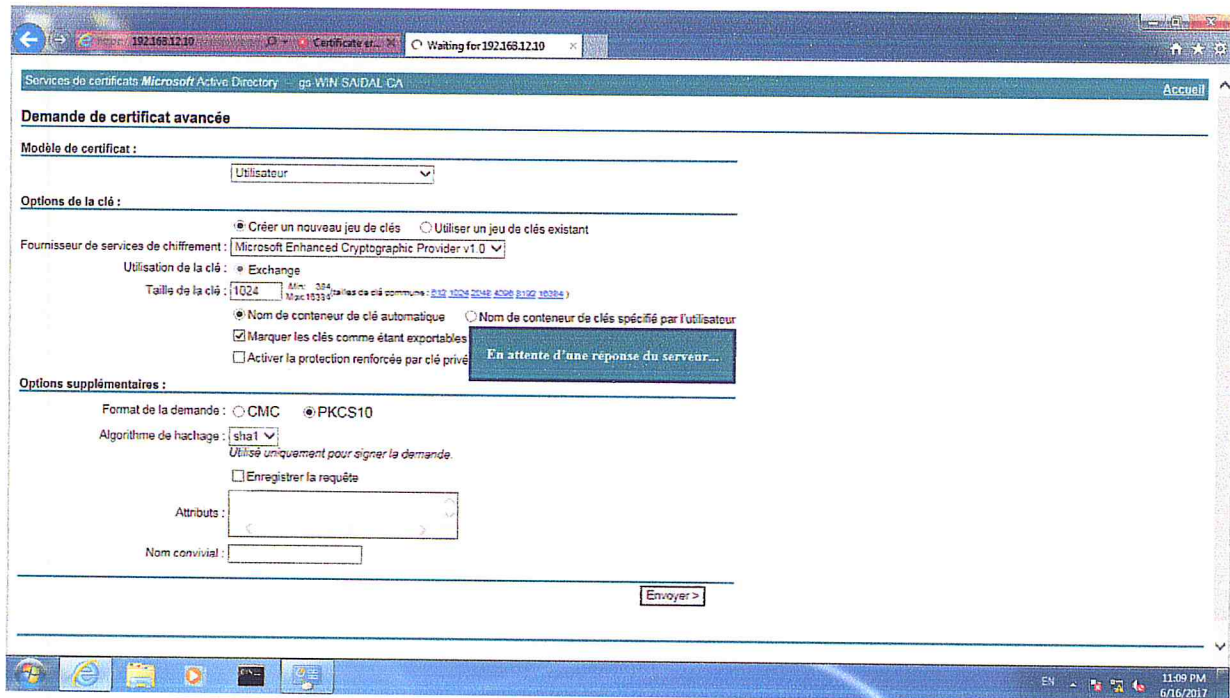
- ❖ Se connecter sur l'ordinateur cible avec un compte du domaine **cfa.est** et lancer une « **console mmc** ».

Cliquer sur « **Fichier** » puis « **Ajouter /Supprimer un composant logiciel enfichable** ». Dans la nouvelle fenêtre, on sélectionne « **Certificats** » puis « **Ajouter** ».

Aller à « **Certificats** » puis cliquer sur le bouton droit sur « **Personnel** », puis Choisir « **Toutes les tâches** » ensuite « **Demander un nouveau Certificat** ».

On suite l'assistant d'installation du Certificat jusqu'à la saisie du nom de L'ordinateur jusqu'à la fin de l'installation.

The screenshot shows the 'Demande de certificat avancée' (Advanced Certificate Request) dialog box in the Microsoft Active Directory Certificate Services console. The dialog is titled 'Demande de certificat avancée' and is part of the 'Services de certificats Microsoft Active Directory' console. The 'Modèle de certificat' (Certificate Template) is set to 'Utilisateur' (User). Under 'Options de la clé' (Key Options), the 'Fournisseur de services de chiffrement' (Cryptographic Service Provider) is 'Microsoft Enhanced Cryptographic Provider v1.0', and the 'Utilisation de la clé' (Key Usage) is 'Exchange'. The 'Taille de la clé' (Key Size) is 1024 bits. The 'Format de la demande' (Request Format) is 'CMC', and the 'Algorithme de hachage' (Hash Algorithm) is 'sha1'. The 'Nom convivial' (Friendly Name) field is empty. The 'Envoyer >' (Send) button is visible at the bottom right of the dialog.



En attente d'une réponse du serveur pour créer une certificat pour l'utilisateur

On peut également examiner sur le serveur, dans « **outils d'administrations/Autorité de certification** » sous « **Certificats délivrés** », tous les certificats que l'autorité de certification a délivré, ainsi que les informations relatives à chaque certificat à savoir :  
l'ID, Nom du demandeur, Modèle de certificat, Date d'effet, date d'expiration, etc....

## INSTALLATION DE NETWORK POLICY SERVER (NPS)

- **Installions du serveur NPS**

Pour installer un serveur radius sur Windows server 2012 r2, il faut installer le rôle NPS (network policy server). Pour cela, il faut suivre les étapes suivantes :

Ouvrir le gestionnaire du serveur, puis cliquer sur « **ajouter des rôles** » et sélectionner « **serveur des stratégies et d'accès réseau** » puis cliquer sur suivant.

## Sélectionner des rôles de serveurs

SERVEUR DE DESTINATION  
server2012.cfa.est

- Avant de commencer
- Type d'installation
- Sélection du serveur
- Rôles de serveurs**
- Fonctionnalités
- Services de stratégie et d'...
- Services de rôle
- Confirmation
- Résultats

Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.

### Rôles

<input type="checkbox"/>	Serveur DNS (Installé)
<input checked="" type="checkbox"/>	Serveur Web (IIS) (16 sur 43 installé(s))
<input checked="" type="checkbox"/>	Services AD DS (Installé)
<input type="checkbox"/>	Services AD FS (Active Directory Federation Service)
<input type="checkbox"/>	Services AD LDS (Active Directory Lightweight Directory Services)
<input type="checkbox"/>	Services AD RMS (Active Directory Rights Management Services)
<input type="checkbox"/>	Services Bureau à distance
<input type="checkbox"/>	Services d'activation en volume
<input type="checkbox"/>	Services d'impression et de numérisation de documents
<input checked="" type="checkbox"/>	Services de certificats Active Directory (2 sur 6 installés)
<input type="checkbox"/>	Services de déploiement Windows
<input checked="" type="checkbox"/>	Services de fichiers et de stockage (2 sur 12 installés)
<input checked="" type="checkbox"/>	Services de stratégie et d'accès réseau
<input type="checkbox"/>	Services WSUS (Windows Server Update Services)

### Description

Les services de stratégie et d'accès réseau fournissent le serveur NPS (Network Policy Server), l'autorité HRA (Health Registration Authority) et le protocole HCAP (Host Credential Authorization Protocol), qui favorisent le maintien de l'intégrité et de la sécurité de votre réseau.

< Précédent

Suivant >

Installer

Annuler

Cocher serveur NPS (network policy server) puis suivant, et terminer l'installation.

## Sélectionner des services de rôle

SERVEUR DE DESTINATION  
server2012.cfa.est

- Avant de commencer
- Type d'installation
- Sélection du serveur
- Rôles de serveurs
- Fonctionnalités
- Services de stratégie et d'...
- Services de rôle**
- Confirmation
- Résultats

Sélectionner les services de rôle à installer pour Services de stratégie et d'accès réseau

### Services de rôle

<input checked="" type="checkbox"/>	Serveur NPS (Network Policy Server)
<input type="checkbox"/>	Autorité HRA (Health Registration Authority)
<input type="checkbox"/>	HCAP (Host Credential Authorization Protocol)

### Description

Le serveur NPS (Network Policy Server) permet de créer et d'appliquer les stratégies d'accès réseau au niveau de l'organisation pour l'intégrité des clients, l'authentification des demandes de connexion et l'autorisation des demandes de connexion. Avec NPS, vous pouvez également déployer la protection d'accès réseau (NAP), une technologie de création, d'application et de mise à jour d'une stratégie d'intégrité client.

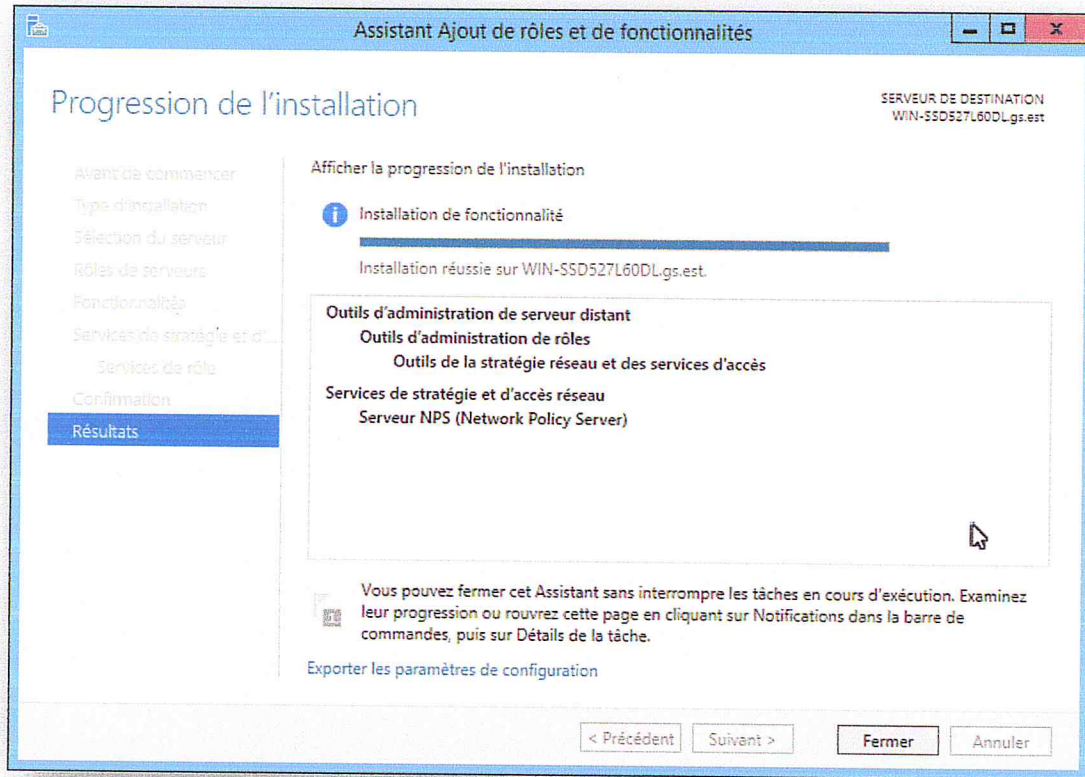
< Précédent

Suivant >

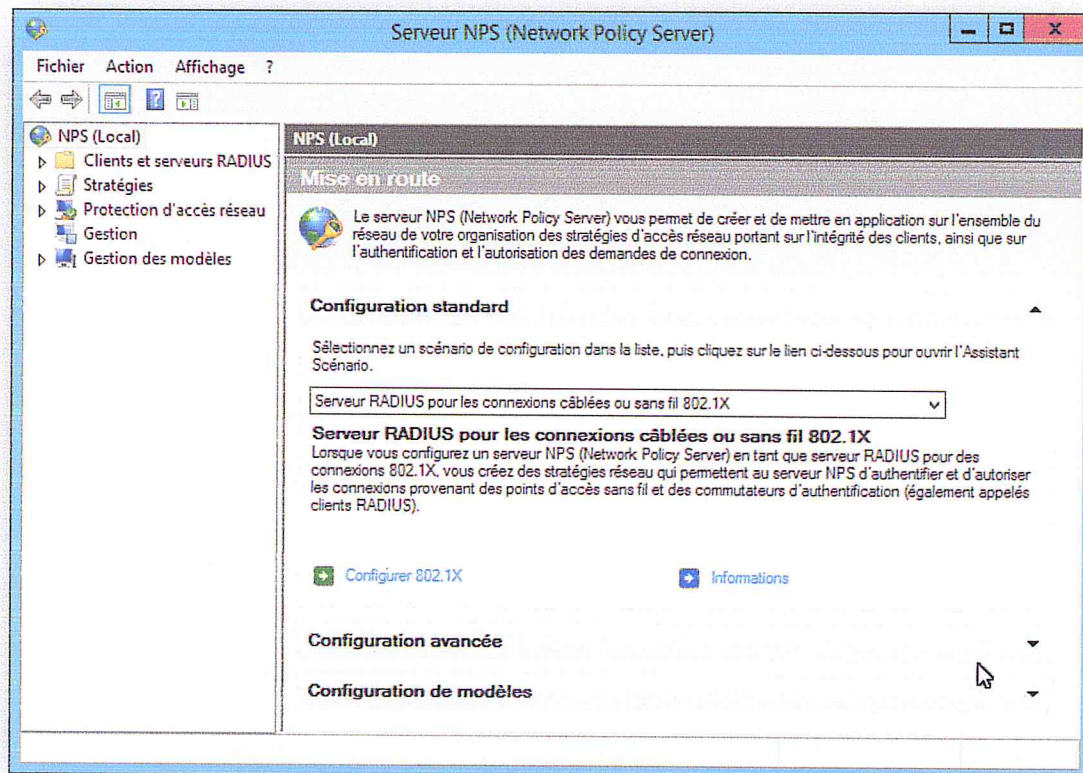
Installer

Annuler

Terminer l'installation du service NPS.



Quand la configuration est terminée, Procédez à l'enregistrement du serveur NPS auprès de l'Active Directory sans quoi il ne pourrait se connecter pour Vérifier les paramètres d'authentification.



- **Ajouter un client RADIUS (SWITCH) :**

Une fois terminé, il faut ajouter le point d'accès (client RADIUS), dans notre cas on utilise un **Switch Cisco 2960**: dans le gestionnaire de serveur développer « **Clients et Serveurs RADIUS** » Faire un clic droit sur « **Clients RADIUS** » puis Choisir « **nouveaux client RADIUS** » en fournissant l'adresse IP ou DNS, nom du fournisseur et le secret partagé (qui sert à la protection des messages échangés entre le client et le serveur).



## Nouveau client RADIUS



### Paramètres

Sélectionner un modèle existant :

### Nom et adresse

Nom convivial :

Adresse (IP ou DNS) :

Vérifier...

### Secret partagé

Sélectionnez un modèle de secrets partagés existant :

Pour taper manuellement un secret partagé, cliquez sur Manuel. Pour générer automatiquement un secret partagé, cliquez sur Générer. Vous devez configurer le client RADIUS avec le même secret partagé entré ici. Les secrets partagés respectent la casse.

Manuel

Générer

Secret partagé :

Confirmez le secret partagé :

OK

Annuler

- **Création des stratégies du réseau**

L'étape suivante consiste à la création d'une stratégie du réseau pour l'équipement support IEEE802.1x. Dans le gestionnaire de serveur développer « **stratégies réseau** » faire un clic droit sur « **nouveaux** » et entrer le nom de la stratégie.

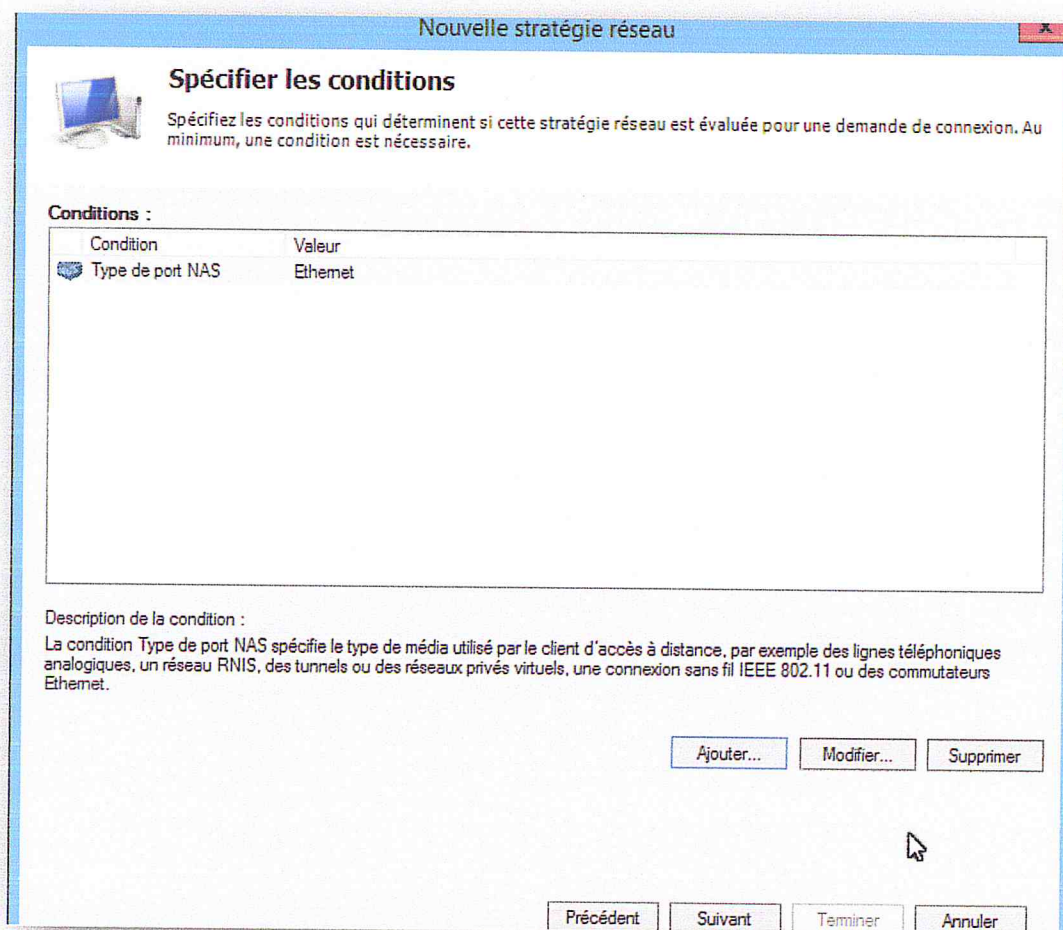
Les stratégies réseau vous permettent d'autoriser les connexions au réseau de manière sélective, et d'indiquer les circonstances dans lesquelles ces connexions peuvent s'effectuer ou non.

Nom de la stratégie	État	Ordre de traitement	Type d'accès	Source
Connexions câblées (Ethernet) sécurisées	Activé	1	Accorder l'accès	Non spécifié
Microsoft de Routage et Accès distants	Activé	999999	Refuser l'accès	Non spécifié
serveurs d'accès	Activé	1000000	Refuser l'accès	Non spécifié

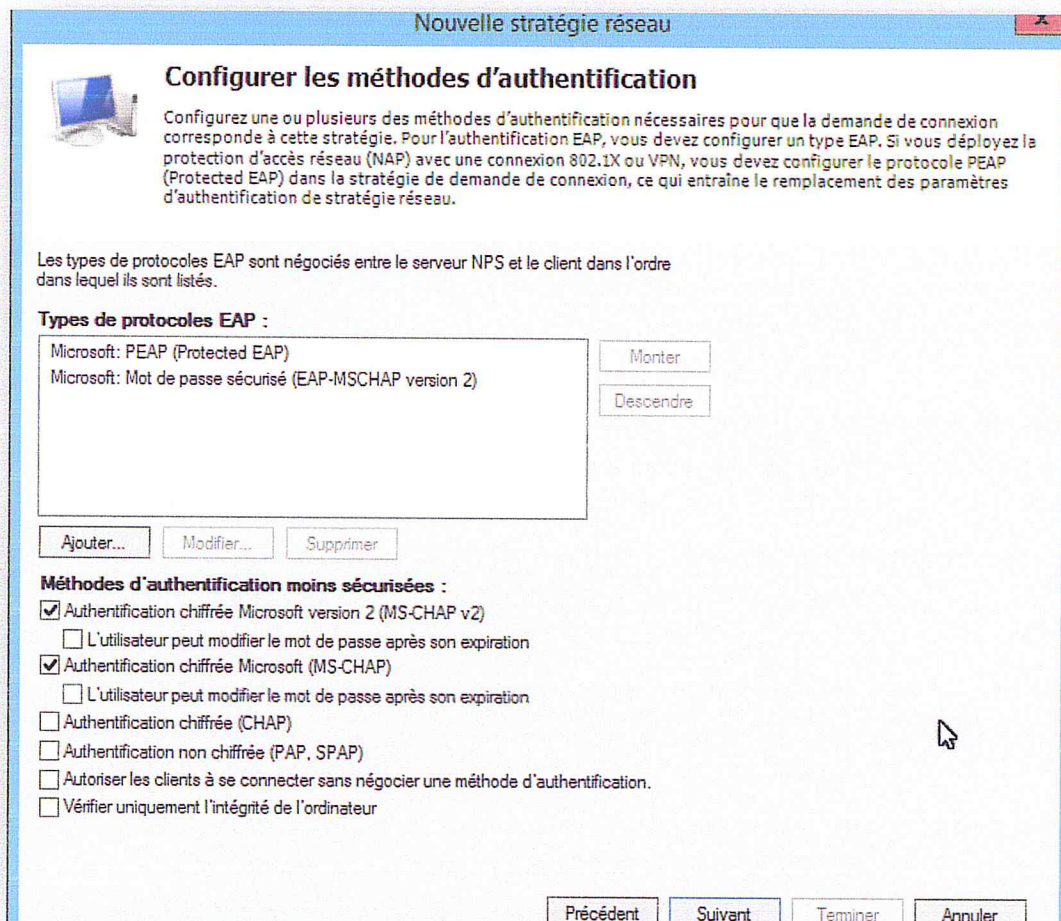
Conditions - Si les conditions suivantes sont réunies :

Condition	Valeur
-----------	--------

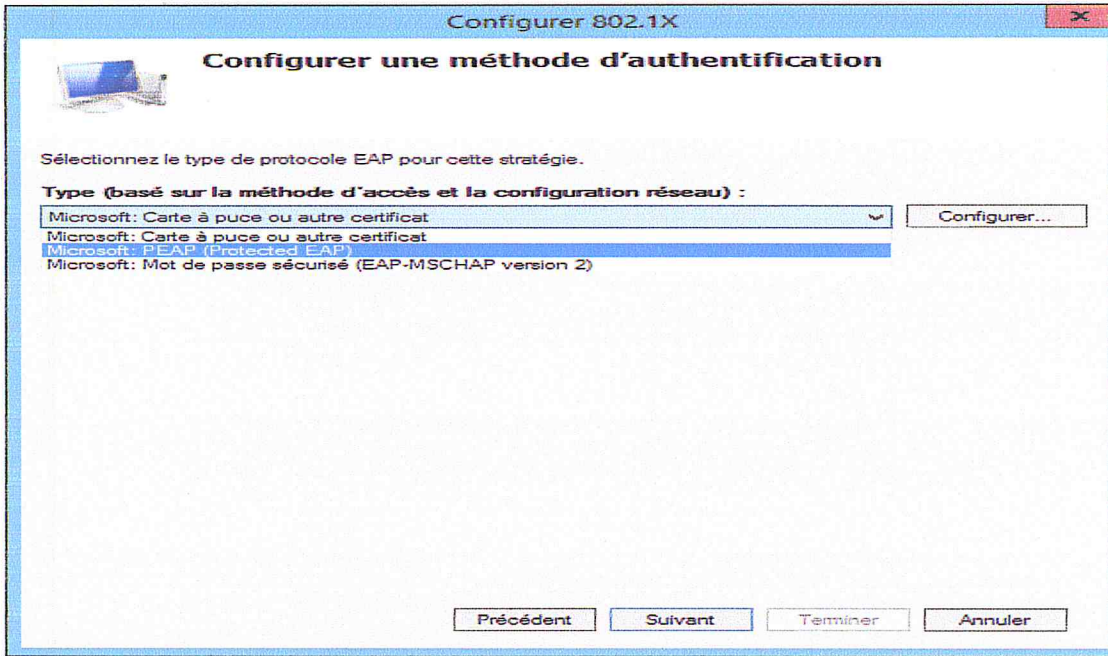
Cliquer sur le bouton « Ajouter », pour ajouter Condition ensuite choisir catégorie « **Type de Port NAS** » Sous type de « **tunnels pour connexions 802.1X standard** » choisir « **Ethernet** » Puis Valider.



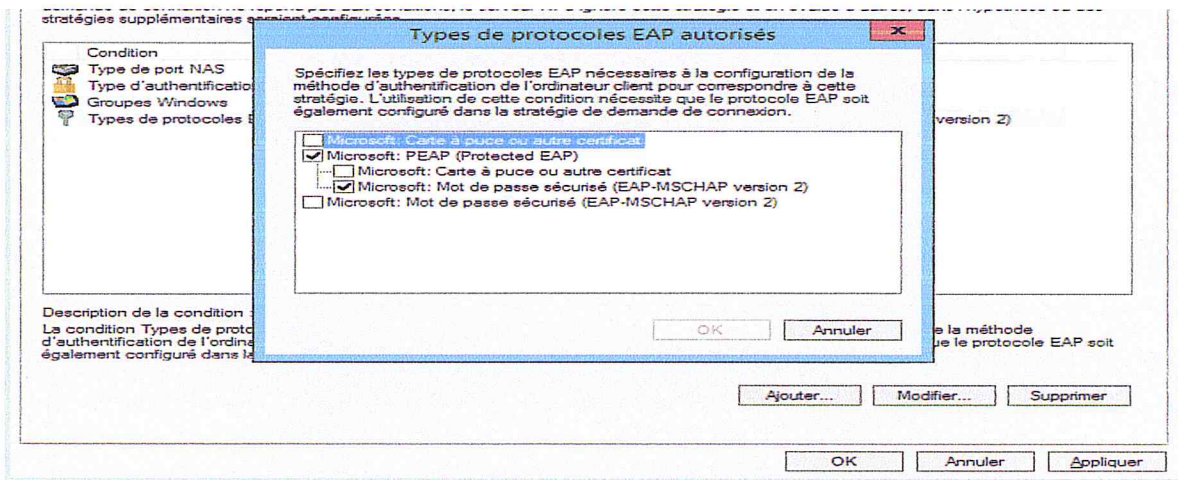
Cliquer sur le bouton « **Ajouter** » pour choisir la catégorie « **Type d'authentification** » et spécifier les méthodes : MS-CHAPv2, PEAP/EAP.



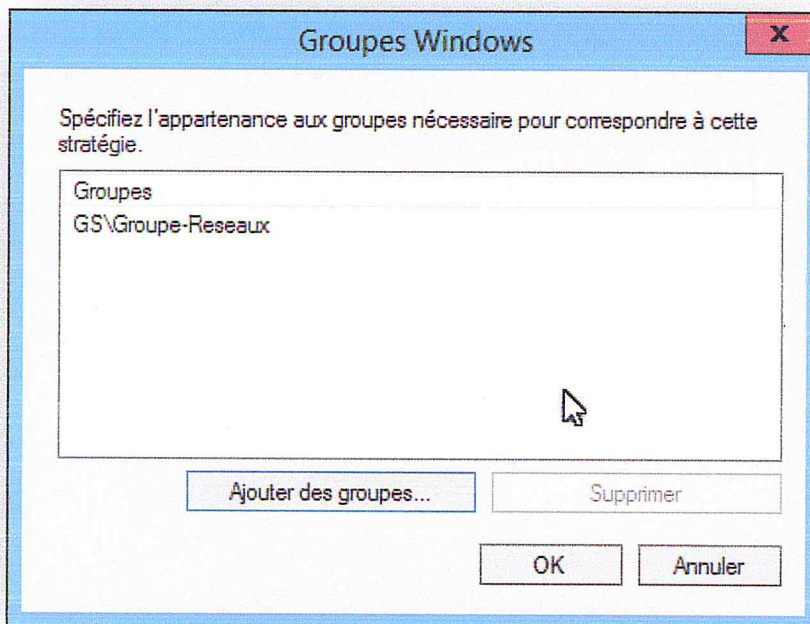
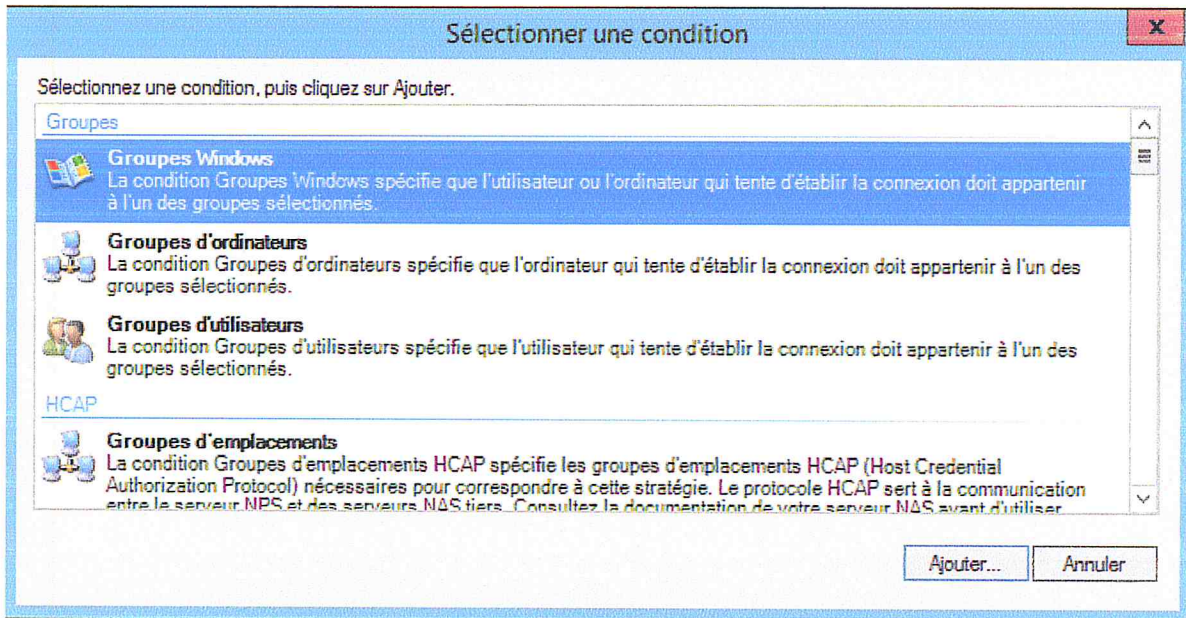
Maintenant il faut choisir quel type d'EAP qui sera utilisé, dans notre cas nous avons choisi « **Microsoft : PEAP protected EAP** ».

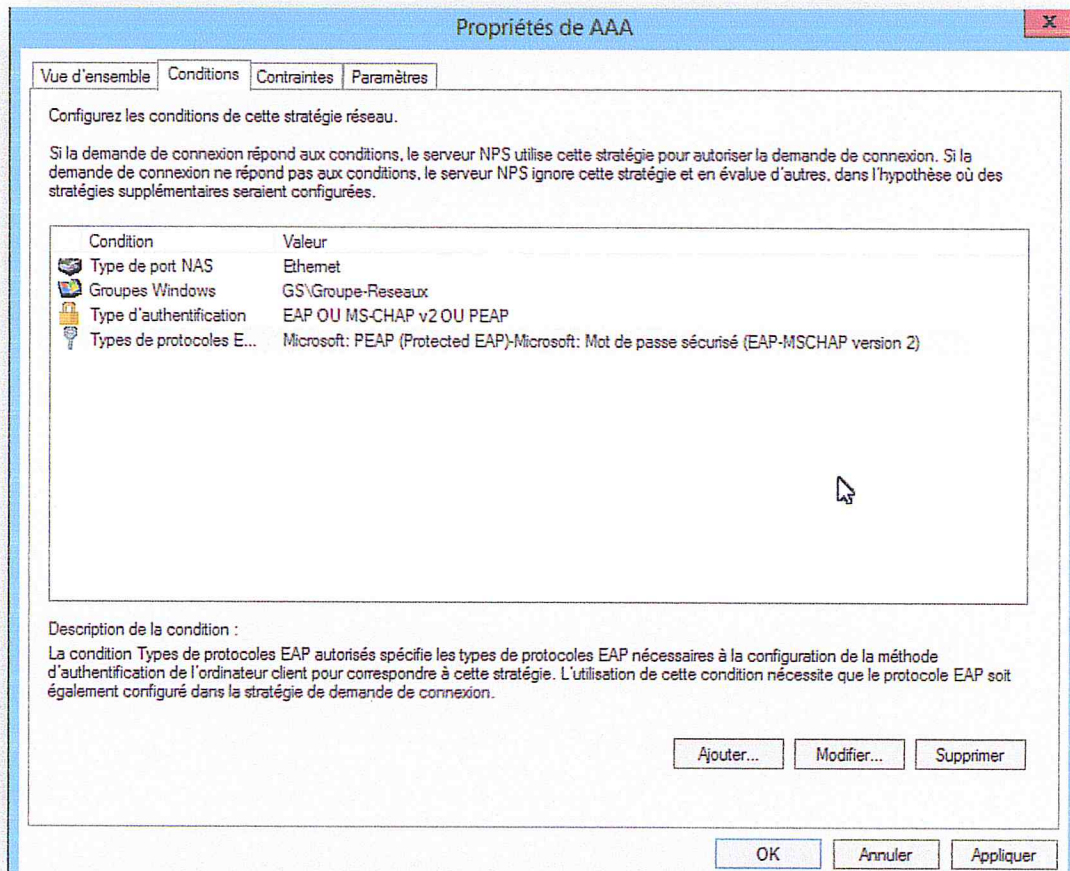


On clique sur « modifier » puis choisir Certificats et type EAP « Mot de passe sécurisé (EAPMSCHAP v2)».



Cliquer sur le bouton « Ajouter » pour choisir la catégorie « Group Windows »





Et a la fin on a la nouvelle stratégie reseau AAA

Serveur NPS (Network Policy Server)

Fichier Action Affichage ?

NPS (Local)

- Clients et serveurs RADIUS
- ▾ Stratégies
  - Stratégies de demande
  - Stratégies réseau
  - Stratégies de contrôle d'accès
- Protection d'accès réseau
- Gestion
- Gestion des modèles

**Stratégies réseau**

Les stratégies réseau vous permettent d'autoriser les connexions au réseau de manière sélective, et d'indiquer les circonstances dans lesquelles ces connexions peuvent s'effectuer ou non.

Nom de la stratégie	État	Ordre de traitement	Type d'accès
Connexions câblées (Ethernet) sécurisées	Activé	1	Accorder l'accès
AAA	Activé	2	Accorder l'accès
Connexions au serveur Microsoft de Routage et Accès distants	Activé	999999	Refuser l'accès
Connexions à d'autres serveurs d'accès	Activé	1000000	Refuser l'accès

AAA

Conditions - Si les conditions suivantes sont réunies :

Condition	Valeur
Type de port NAS	Ethernet
Groupes Windows	GS\Groupe-Reseaux
Type d'authentification	EAP OU MS-CHAP v2 OU PEAP
Types de protocoles EAP autorisés	Microsoft: PEAP (Protected EAP)-Microsoft: Mot de passe sécurisé (EAP...)

Paramètres - Les paramètres suivants sont appliqués :

Paramètre	Valeur
Méthode d'authentification	Protocole EAP OU MS-CHAP v1 OU MS-CHAP v2
	III



## CONFIGURATION DU SWITCH D'ACCÈS

La configuration des clients Radius qui sont dans notre projet des commutateurs d'accès nécessite les étapes suivantes :

- **Une Configuration Initiale Sur Le Commutateur D'accès Tel Que Les Mots De Passe D'accès :**

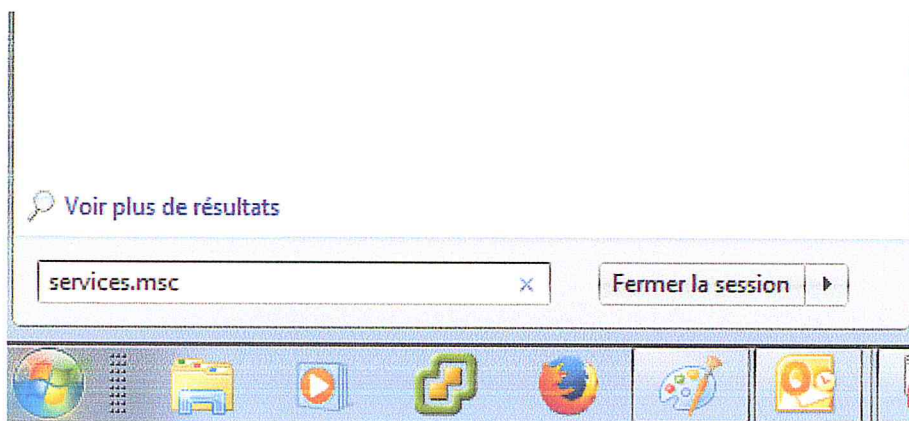
```
hostname client_Radius
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$HGvO$Y3CaLRigKJR6UhtqdU2rC.
enable password 7 0301481F545F701A04
!
line con 0
exec-timeout 0 0
privilege level 15
password 7 121C1603405B5D5260
logging synchronous
line vty 0 4
password 7 09495D1D4B55464441
```

- **La Création Des Vlan Et L'affectation Des Ports De Connexion Aux Vlan De Travail .**
- **Configuration Des Service AAA .**
- **Configuration Des Ports .**

## CONFIGURATION DU CLIENT SUPPLICANT

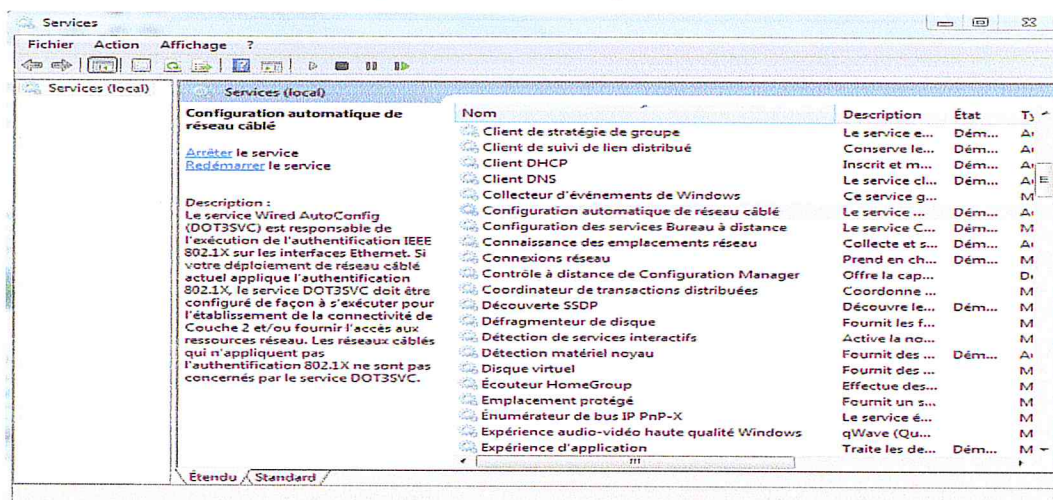
- Configuration d'une connexion Client filaire sous Windows7 :

Inscrivez `services.msc` Dans le champ de saisie Rechercher les programmes et fichiers À partir du menu Démarrage Windows

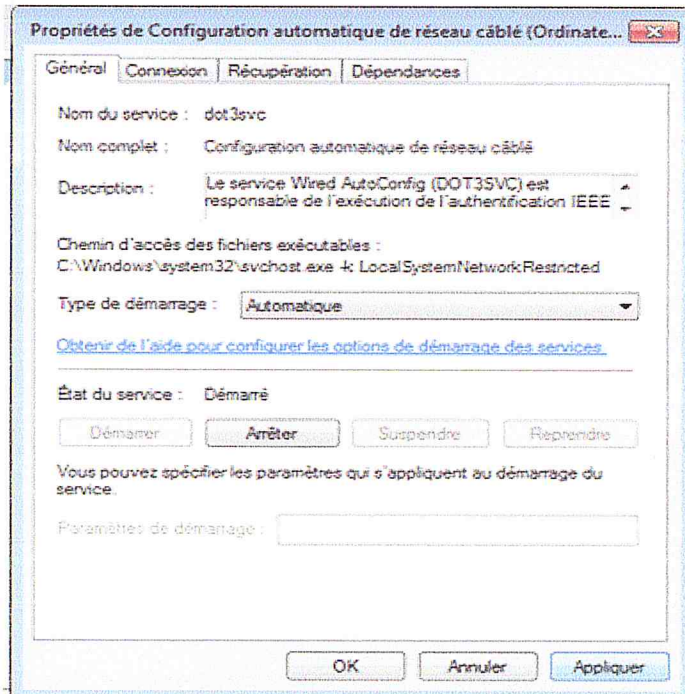


Démarrage du service d'authentification 802.1X

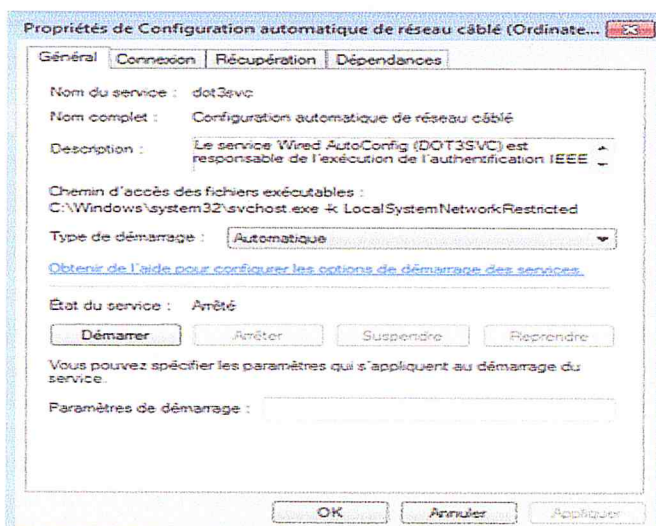
Sélectionnez le service Configuration automatique du réseau câblé



Au menu déroulant "**Type de démarrage**" sélectionnez le type **Automatique** et cliquez sur le bouton **Appliquer**



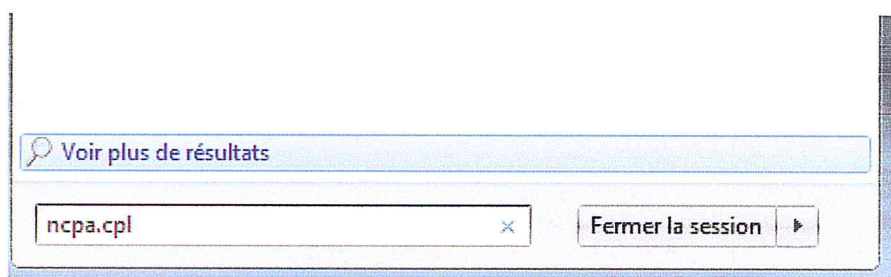
A la section sur l'**État du service**, cliquez sur le bouton **Démarrer** et par la suite sur le bouton **OK**



Fermez la fenêtre des Services Windows.

- **Activation et configuration de l'authentification 802.1X**

Inscrivez **NCPA.CPL** dans le champ de saisie Rechercher les programmes et fichiers, À partir du menu Démarrage Windows



Sélectionnez la **connexion au réseau local** de votre poste et sélectionnez **Propriétés** à l'aide du menu bouton droit de la souris.

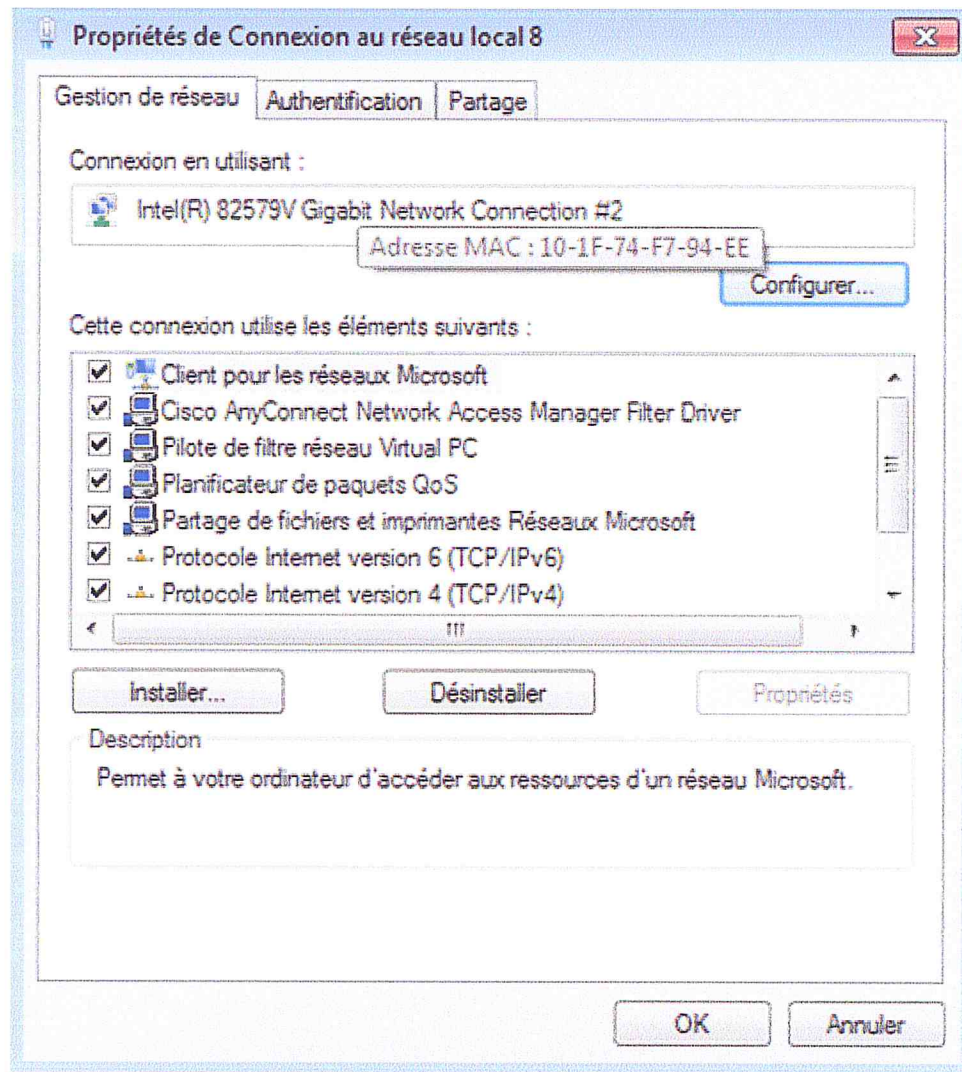
Fichier Edition Affichage Outils Avancé ?  
Organiser ▼ Désactiver ce périphérique réseau Diagnostiquer cette

Connexion au réseau local  
ads.umontreal.ca  
Intel(R) 82579LM Gigabit N

UdeM  
Non disponible

- Désactiver
- Statut
- Diagnostiquer
- Connexions de pont
- Créer un raccourci
- Supprimer
- Renommer
- Propriétés

Sélectionnez l'onglet **Authentification**



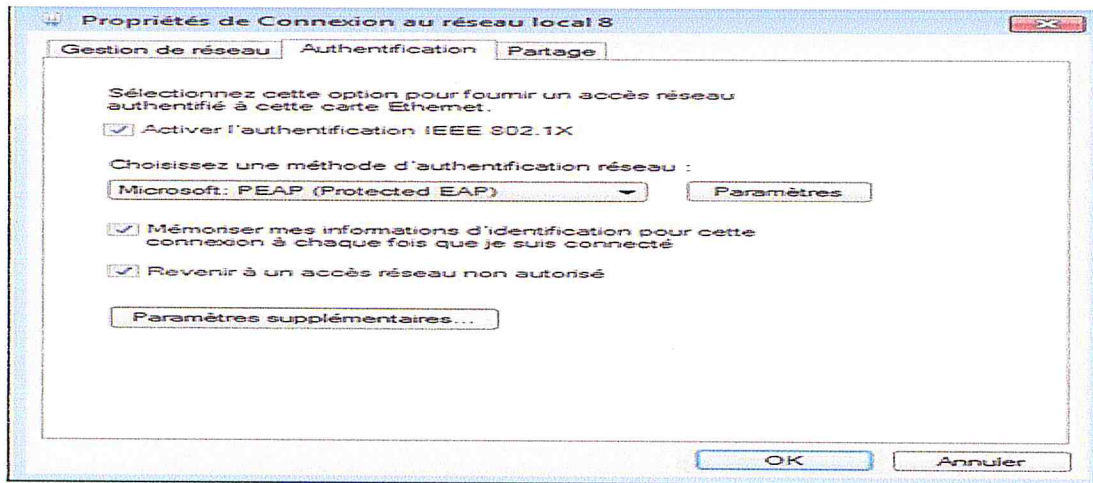
Cochez la case **Activer l'authentification IEEE 802.1X**

- À partir du menu déroulant "**Choisissez une méthode d'authentification réseau**", sélectionnez **Microsoft: PEAP**

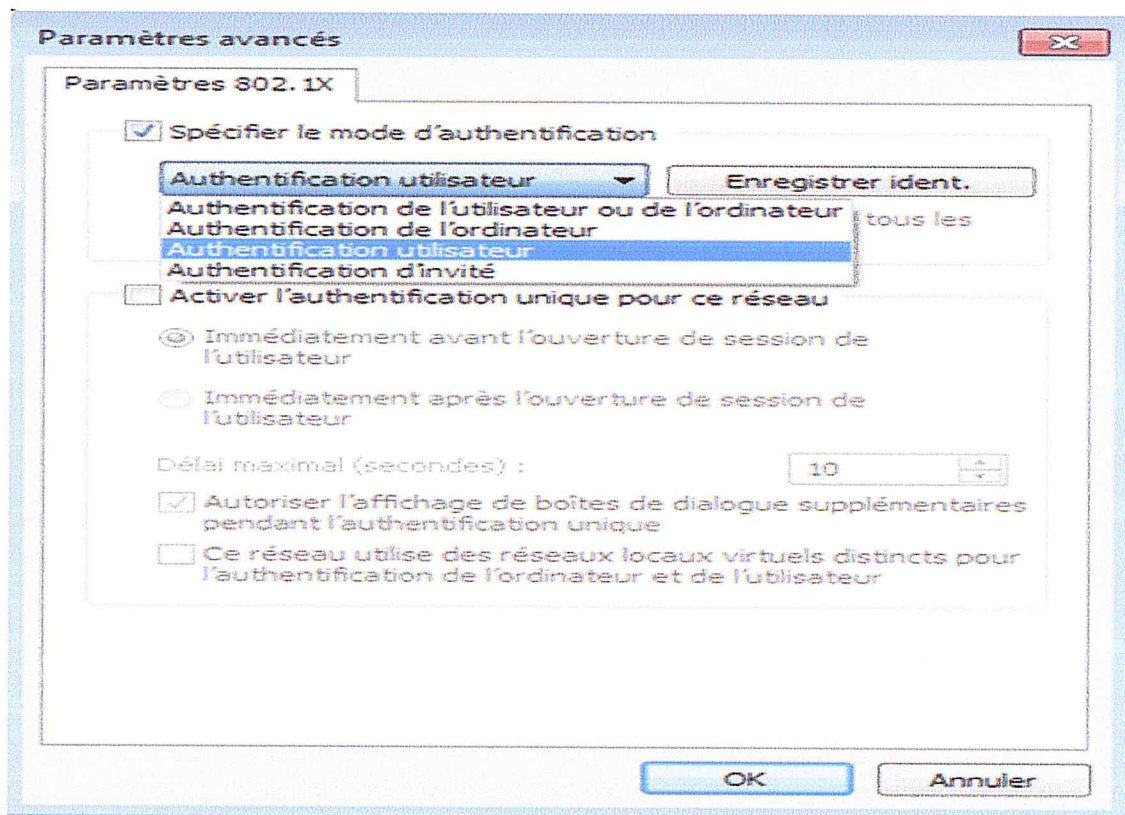
- Cochez la case **Mémoriser mes informations d'identification** pour cette connexion à chaque fois que je suis connecté

- Cochez la case **Revenir à un accès réseau non autorisé**

- Cliquez sur **Paramètres Supplémentaires**



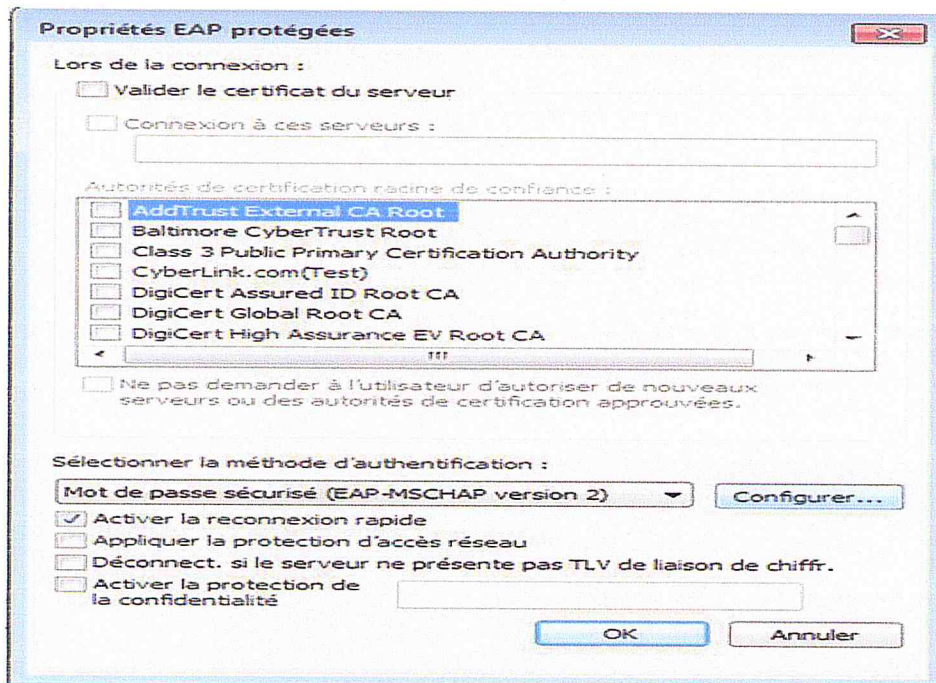
- Cochez la case **Spécifier le mode d'authentification** et sélectionnez **Authentification utilisateur**. Cliquez sur le bouton OK



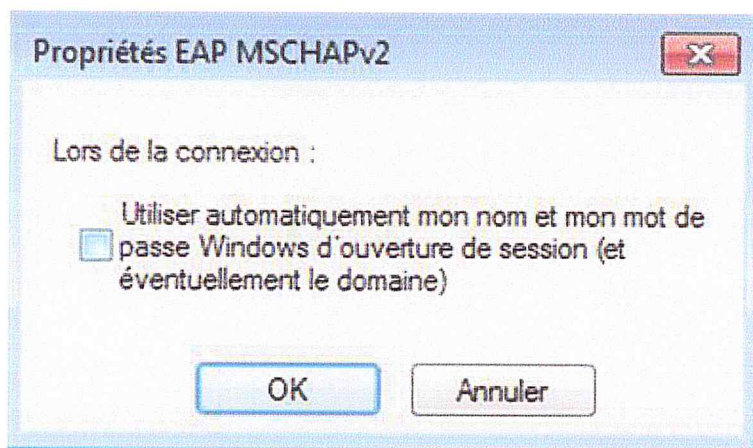
- De retour à la fenêtre "**Propriété de connexion au réseau local**", cliquez sur le bouton **Paramètres**

- À partir du menu déroulant "Sélectionner la méthode d'authentification", sélectionnez l'option **Mot de passe sécurisé (EAP-MSCHAP version 2)**

- Cliquez sur le bouton **Configurer**



- Assurez-vous que la case de la fenêtre "Propriétés EAP MSCHAPv2" n'est PAS cochée. Cliquez sur le bouton OK



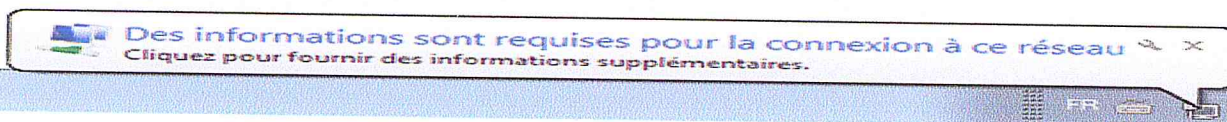
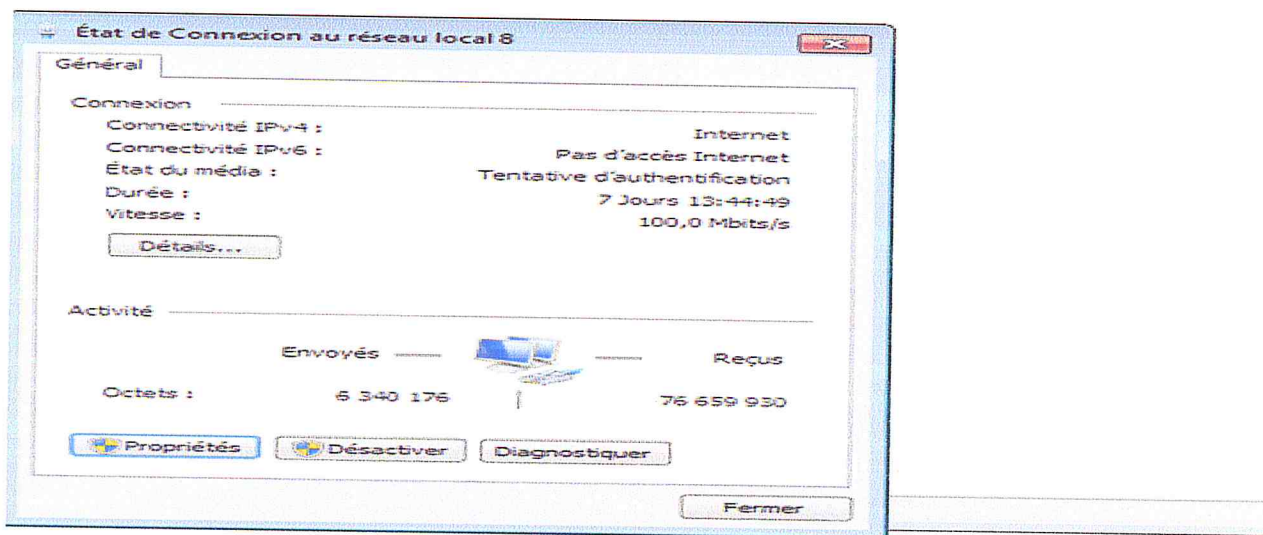


- De retour à la fenêtre "**Propriétés EAP protégées**", cochez la case **Activer la reconnexion rapide** et cliquez sur le bouton OK (voir image précédente).

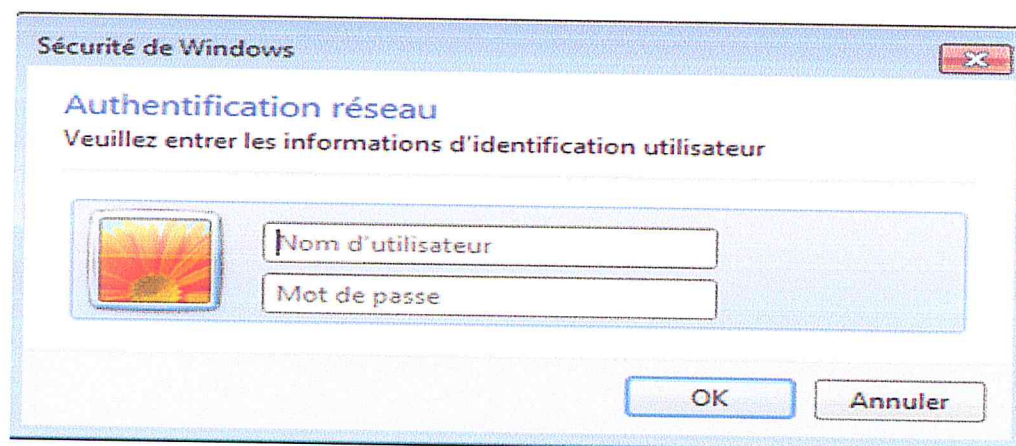
- De retour à la fenêtre des **propriétés de la connexion réseau locale**, cliquez sur le bouton OK pour fermer la fenêtre.

- **Connexion au réseau filaire**

Suite à ces opérations, un message d'information sera affiché au bas de l'écran vous avisant que Des informations sont requises pour la connexion à ce réseau. Cliquez sur le lien de ce message.



- Saisissez vos identifiants SIM et cliquez sur le bouton OK.



Vous serez connecté au réseau filaire dans la communauté utilisateur correspondante.

- **Configuration d'une connexion Client filaire sous Windows 8**
1. tapez **services.msc** Dans le champ de saisie Rechercher les programmes et fichiers et puis cliquez sur **OK**.
  2. Clic droit sur **Configuration automatique du réseau câblé** . Choisissez **Propriétés** dans le menu contextuel.
  3. Modifier le type de démarrage sur **Automatique** et cliquez sur **Démarrer**. Suivez en cliquant sur **OK**
  4. Maintenez le bouton de **fenêtre-clé** et appuyez sur **R**, le **contrôle de type** et cliquez sur **OK**.
  5. Clic droit sur **Connexion au réseau local (Ethernet)**. Choisissez **Propriétés** dans le pop up menu.
  6. Cliquez sur l'onglet **Authentification**. Cochez **Activer l'authentification IEEE 802.1X**. Vérifier "**Rappelez- vous mes informations d'identification pour cette connexion chaque fois que je suis connecté**". Vérifiez « se retirer à l'accès non autorisé au réseau ». Choisissez **Microsoft PEAP (Protected EAP)** en tant que **réseau Méthode d'authentification**. Ensuite, cliquez sur **Paramètres**.
  7. Cochez l'option «**Vérifier l'identité du serveur en validant le certificat**» et "**Connexion à ces serveurs** ".
  8. Cochez la case "**Activer reconnexion rapide**". Option Décochez "**Application Network Access Protection**", et "**Activer Identité confidentialité** " Choisissez un mot de passe sécurisé (**EAP-MSCHAP v2**) comme **méthode d'authentification**. Puis clique **Configurer**.
  9. Si ceci est un ordinateur de domaine, cochez l'option "**Utiliser automatiquement mon nom d'ouverture de session Windows et mot de passe** (et éventuellement le domaine) ". Puis cliquez sur **OK**.
  10. À son retour au menu «**Propriétés EAP protégées**», cliquez sur **OK**.
  11. Cliquez sur **Paramètres supplémentaires**.
  12. Vérifiez Spécifiez le **mode d'authentification**, Sélectionner un **utilisateur** ou **l'authentification de l'ordinateur** à partir du dans le menu déroulant, puis cliquez sur **OK**.
  13. Cliquez sur **OK**.

14. Une fois connecté au port câblé, vous serez en mesure d'obtenir la fenêtre d'authentification réseau.
15. Entrez **Nom d'utilisateur** (Domain \ Nom d'utilisateur ) et **mot de passe**, puis cliquez sur **OK**.
16. Une fois l'authentification, l'utilisateur sera connecté avec succès au réseau.

