# DOCUMENTATION TECHNIQUE

Mise en place de Wifi d'entreprise via un serveur de domaine avec Active Directory, DHCP, DNS et NPS

> Lionel Baptiste Epreuve E4 – Situation professionnelle Session : 2016

### Table des Matières

ТАВ	LE DES MATIERES	1
ТАВ	LE DES FIGURES	2
1.	INTRODUCTION	3
2.	PREREQUIS	4
A B	<ul> <li>CONFIGURATION DES MACHINES HOTES</li> <li>CONFIGURATION DES MACHINES VIRTUELLES</li> </ul>	4 4
3. BOR	INSTALLATION ET CONFIGURATION DU SERVEUR D'AUTHENTIFICATION ET DE LA	6
A)	INSTALLATION ET CONFIGURATION DU ROLE SERVICES DE CERTIFICATS ACTIVE DIRECTORY	6
в)	INSTALLATION ET CONFIGURATION DU SERVICES DE STRATEGIE ET D'ACCES RESEAU	· 11
c)	CONFIGURATION DES PROPRIETES DES UTILISATEURS DE L'ACTIVE DIRECTORY	· 17
D)	) Mise en place d'une strategie de groupe	- 18
E)	CONFIGURATION DU POINT D'ACCES WIFI WRT54GL	· 23
4.	CONCLUSION	27

## Table des Figures

Figure 1 : Serveur 2012 M2L	6
Figure 2 : Ajout du rôle Services de certificats Active Directory	7
Figure 3 : Autorité de certification	7
Figure 4 : Configuration des services de certificats	8
Figure 5 : Autorité de certification d'entreprise	8
Figure 6 : Choix de l'algorithme de chiffrement	9
Figure 7 : Nom de l'AC	9
Figure 8 : Emplacement des bases de données	10
Figure 9 : Autorité de certification fonctionnelle	10
Figure 10 : Ajout des Services de stratégies d'accès réseau	11
Figure 11 : Réservation IP dans le serveur DHCP	11
Figure 12 : Configuration 802.1X	12
Figure 13 : Connexions sans fil sécurisées	12
Figure 14 : Ajout d'un client Radius	13
Figure 15 : Configuration du type de protocole EAP pour la stratégie	14
Figure 16 : Sélection du certificat	14
Figure 17 : Groupe pour la stratégie	14
Figure 18 : Inscription d'un serveur dans l'AD	15
Figure 19 : Inscription du serveur dans l'AD	15
Figure 20 : Configurer la gestion des comptes	
Figure 21 : Enregistrement des données sur le PC	
Figure 22 : Journalisation dans un fichier local	17
Figure 23 : Appel entrant	
Figure 24 : Ajout dans le groupe Uti-WIFI	
Figure 25 : Stratégie de groupe	
Figure 26 : Stratégie de réseau sans fil	19
Figure 27 : Configuration de la stratègie de rèseau sans fil	19
Figure 28 : Sécurité de la stratègie	20
Figure 29 : Autorisation de la strategie	
Figure 30 : Création d'une stratègie Win XP	
Figure 31 : Les deux stratégie d'accès réseau	
Figure 32 : Ma nouvelle GPO Active	
Figure 33 : Configuration reseau + relay DHCP	23
Figure 34 : Configuration WIFI de base	24
Figure 35 : Configuration Radius	
Figure 36 : Configuration de la sécurité sans fil	26

#### 1. Introduction

Dans ce projet, je décide de mettre en place une connexion Wifi d'entreprise sécurisée. Deux solutions s'offrent à moi pour mener à bien ce projet :

#### Un réseau de hot spot :

Un réseau hot spot est totalement distinct de celui de l'entreprise. Il est généralement constitué d'un réseau de bornes Wi-Fi connectées à une application spécialisée (Bluesocket, Nomadix, etc.) ou à un serveur dédié équipé d'un logiciel de gestion des hot spots (Ucopia, Netinary, etc.).

Cet équipement se charge d'authentifier les utilisateurs sans aucun lien avec le référentiel de l'entreprise. Il ne présume par ailleurs d'aucun type d'adressage et s'adapte à ce que lui envoie le client dès la connexion à la borne, au niveau 2 de la couche réseau. À ce stade, le client est sur un portail web captif et l'utilisateur ne peut que saisir un identifiant. Il s'agit généralement du couple "login/mot de passe "défini sur l'équipement lui-même ou éventuellement stocké dans l'annuaire LDAP de l'entreprise, dans un profil visiteur par exemple.

Une fois authentifié, l'accès est ouvert vers internet et la connexion entre le client et la borne est généralement chiffrée grâce au standard de sécurité WPA (dont la clé est fournie via le protocole 802.1x), ou grâce à du WEP dynamique pour les clients qui ne supporteraient pas le WPA. Selon les équipements, il est également possible de définir des niveaux de qualité de service, par exemple, pour ces connexions.

#### Un serveur NPS / Radius :

Cela doit offrir un accès complet au système d'information de l'entreprise : un choix plus risqué. En contrepartie les utilisateurs sont connus et la configuration des clients mieux maîtrisée, permettant une plus grande souplesse dans l'authentification et la sécurité.

L'architecture est toutefois plus complexe : les bornes doivent relayer l'authentification des clients au mécanisme existant de l'entreprise, généralement un annuaire LDAP ou Active Directory. Hélas, en matière d'authentification, les bornes Wi-Fi ne comprennent nativement que le protocole 802.1x, qui lui-même ne parle qu'aux serveurs Radius.

#### Solution retenue :

L'élément essentiel est de déterminer à qui va servir le Wi-Fi, étant donné que ce sont les utilisateurs de mon précédent projet qui portait sur l'installation d'un serveur de domaine avec Active Directory, DHCP et DNS sous Windows Serveur 2012, je décide de mettre en place une serveur NPS, Network Policy Server. Il aura pour but de d'authentifier les utilisateurs via le login et password des utilisateurs de l'AD.

Sur mon ordinateur, là où j'ai ma machine virtuelle du serveur, je vais rajouter le service NPS pour initialiser un serveur Radius. Ensuite je configurerai mon point accès Wifi en fonction de ce serveur. Afin que les utilisateurs de la Maison des Ligues puissent avoir accès au Wifi sans rien faire, je vais ensuite créer une GPO qui aura pour but de paramétrer l'authentification via mon serveur Radius.

#### 2. Prérequis

Pour mettre en place ce projet, je vais avoir besoin de ma machine virtuelle sous Windows Serveur 2012 ainsi que d'une machine sous Windows 7 sur mon domaine et muni d'un adaptateur Wifi.

Mon serveur de domaine étant déjà configuré en fonction du contexte M2L, je n'ai juste à y installer mes nouveaux services et les configurer.

Il sera nécessaire d'avoir un point d'accès Wifi compatible avec un serveur Radius et le protocole 802.1x. Pour ça je vais utiliser l'AP « Linksys by cisco ; WRT54GL ». Attention pour que la borne soit compatible il faut qu'elle ait un firmware de cette distribution dd-wrt.com que j'aurais au préalable flashé.

Je récupère donc les configurations machines de mon précédent projet qui sont les suivantes :

#### A) Configuration des machines hôtes

#### Ordinateur fixe :

- Système d'exploitation : Windows 7 64 bits
- Mémoire vive : 16Go
- Disque dur : 1To
- Processeur : Intel Core i5-4690 CPU @3.50GHz-3.50GHz

#### Ordinateur fixe :

- Système d'exploitation : Windows 7 64 bits
- Mémoire vive : 8Go
- Disque dur : 1To
- Processeur : Intel Core i7-4510U CPU @2.00GHz 2.60GHz

#### B) Configuration des machines virtuelles

#### Ordinateur fixe :

Machine Virtuelle 1 :

- Nom : WIN2012-M2L
- Système d'exploitation : Windows serveur 2012 R2
- Processeur : Intel Core i5-4690 CPU @3.50GHz-3.50GHz
- Mémoire vive : 3Go
- o Disque dur : 25Go

- Nombre d'interface : 1
- o Mode accès réseau : Accès par pont

Machine Virtuelle 2 :

- Nom : IPCOP
- Système d'exploitation : IPCop-2.1.8
- Processeur : Intel Core i5-4690 CPU @3.50GHz-3.50GHz
- Mémoire vive : 1Go
- Disque dur : 8Go
- Nombre d'interface : 2
- Mode accès réseau :
  - Interface 1 : Réseau privé hôte
  - Interface 2 : Accès par pont

#### Ordinateur portable :

Machine Virtuelle Cliente :

- $\circ$  Nom : Windows7
- Système d'exploitation : Windows 7 Professionnel SP1
- Processeur : Intel Core i7-4510U CPU @2.00GHz 2.60GHz
- Mémoire vive : 4Go
- Disque dur : 35Go
- Nombre d'interface :
- Mode d'accès réseau : Accès par pont

#### 3. Installation et configuration du serveur d'authentification et de la borne WIFI

Je commence par redémarrer mon serveur Windows Serveur 2012 R2 sur mon ordinateur fixe par le biais de VM VirtualBox.





Afin de mettre en œuvre le serveur d'authentification il est nécessaire d'avoir les services suivants :

- Autorité de certification (certificat serveur)
- Serveur Radius (NPS)
- a) Installation et configuration du rôle Services de certificats Active Directory

Donc pour ça je fais « Gérer », je clique sur « ajouter des rôles et fonctionnalités », je choisis I'« Installation basée sur un rôle ou une fonctionnalité » et je fais suivant. J'ajoute ensuite le rôle « Services de certificats Active directory ».

È.	Assistant Ajout de rôles et de fonctionnalités	_ <b>D</b> X
Sélectionner des r	rôles de serveurs	SERVEUR DE DESTINATION WIN2012-M2LM2Llocal
Avant de commencer	Sélectionnez un ou plusieurs rôles à installer sur le serveur sélec	tionné.
Type d'installation	Rôles	Description
Sélection du serveur	······································	Les services de certificats Active
Rôles de serveurs	Serveur DNS (Installé)	Directory (AD CS) servent à créer des
Fonctionnalités	Serveur Web (IIS)	autorités de certification et les services de rôle associés pour
AD CS	Services AD DS (Installé)	émettre et gérer les certificats
Services de rôle	Services AD FS (Active Directory Federation Service	utilisés dans diverses applications.
Confirmation	Services AD EDS (Active Directory Lightweight Dire	
Résultats	Services Bureau à distance	
	Services d'activation en volume	
	Services d'impression et de numérisation de docu	
	Services de certificats Active Directory	
	Services de déploiement Windows	
	Services de fichiers et de stockage (2 sur 12 install	
	Services de stratégie et d'accès réseau	
	Services WSUS (Windows Server Update Services)	
	< Précédent Suivant	t > Installer Annuler

Figure 2 : Ajout du rôle Services de certificats Active Directory

Je laisse les valeurs par défaut et je fais Installer.

2	Assistant Ajout de rôles et de fonctionnalités	_ <b>_</b> X
Sélectionner des s Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités AD CS Services de rôle Confirmation Résultats	Assistant Ajout de rôles et de fonctionnalités Services de rôle Sélectionner les services de rôle à installer pour Services de cer Services de rôle Autorité de certification Inscription de l'autorité de certification via le Web Répondeur en ligne Service d'inscription de périphérique réseau Service Web Inscription de certificats Service Web Stratégie d'inscription de certificats	SERVEUR DE DESTINATION WIN2012-M2LM2LIocal tificats Active Directory Description Une autorité de certification sert à émettre et gérer des certificats. Plusieurs autorités de certification peuvent être liées pour former une infrastructure à clé publique.
	< Précédent Suiva	nt > Installer Annuler

Figure 3 : Autorité de certification

7

\_\_\_\_\_

Je choisis maintenant de configurer les services de certificats.

<b>a</b>	Gestionnaire de serveur	x
€ • • Tab	eau de bord 🔹 🕄   🍢 Gérer Outils Afficher Aide	2
<ul> <li>Tableau de bord</li> <li>Serveur local</li> <li>Tous les serveurs</li> <li>AD CS</li> <li>AD DS</li> <li>DHCP</li> <li>DNS</li> <li>Services de fichiers et d</li> </ul>	<ul> <li>Configuration post-déploie</li> <li>Configuration requise pour : Services de certificats Active Directory à WIN2012-M2L</li> <li>Configurer les services de certificats Active Director</li> <li>Installation de fonctionnalité</li> <li>Configuration requise. Installation réussie sur WIN2012-M2L.local.</li> <li>Ajouter des rôles et fonctionnalités</li> <li>Détails de la tâche</li> </ul>	
	Rôles et groupes de serveurs       Rôles : 5   Groupes de serveurs : 1   Nombre total de serveurs : 1       Image: AD CS     1	~

Figure 4 : Configuration des services de certificats

Ici je choisis « Autorité de certification d'entreprise ».

E C	onfiguration des services de certificats Active Directory
Type d'installation	SERVEUR DE DESTINATION WIN2012-M2L.M2L.local
Services de rôle Type d'installation	Les autorités de certification d'entreprise peuvent utiliser les services de domaine Active Directory
Type d'AC Clé privée	(AD DS) pour simplifier la gestion des certificats. Les autorités de certification autonomes n'utilisent pas AD DS pour émettre ou gérer des certificats.
Chiffrement Nom de l'AC	<ul> <li>Autorité de certification d'entreprise</li> <li>Les autorités de certification d'entreprise doivent être membres d'un domaine et sont généralement en ligne pour émettre des certificats ou des stratégies de certificat.</li> </ul>
Période de validité Base de données de certi Confirmation Progression Résultats	Autorité de certification autonome Les autorités de certification autonomes peuvent être membres d'un groupe de travail ou d'un domaine. Les autorités de certification autonomes ne nécessitent pas AD DS et peuvent être utilisées sans connexion réseau (hors connexion).
	En savoir plus sur le type d'installation
	< Précédent Suivant > Configurer Annuler

Figure 5 : Autorité de certification d'entreprise

Je laisse les valeurs par défaut et je fais suivant, ensuite je choisis l'algorithme « **SHA1** ». Puis je fais suivant.

<b>b</b> (	Configuration des services de certificats Active Director	у	_ <b>D</b> X
Chiffrement pour	l'autorité de certification		SERVEUR DE DESTINATION WIN2012-M2L.M2L.local
Informations d'identificati Services de rôle	Spécifier les options de chiffrement		
Type d'installation	Sélectionnez un fournisseur de chiffrement :		Longueur de la clé :
Type d'AC	RSA#Microsoft Software Key Storage Provider	•	2048 🔻
Clé privée Chiffrement Nom de l'AC Période de validité Base de données de certi Confirmation Progression Résultats	Sélectionnez l'algorithme de hachage pour signer les certificats ér SHA256 SHA384 SHA512 SHA1 Autorisez l'interaction de l'administrateur lorsque l'autorité de privée.	mis	par cette AC : tification accède à la clé
	En savoir plus sur le chiffrement		
	< Précédent Suivant >		Configurer Annuler

*Figure 6 : Choix de l'algorithme de chiffrement* 

Je nomme l'Autorité de Certification.

Spécifier le nom de l'AC
Tapez un nom commun pour identifier cette autorité de certification. Ce nom est ajouté à tous les certificats émis par l'autorité de certification. Les valeurs des suffixes du nom unique sont générées automatiquement, mais elles sont modifiables.
Nom commun de cette AC :
M2L-WIN2012-M2L-CA
Suffixe du nom unique :
DC=M2L,DC=local
Aperçu du nom unique :
CN=M2L-WIN2012-M2L-CA,DC=M2L,DC=local
En savoir plus sur le nom de l'autorité de certification
< Précédent Suivant > Configurer Annuler
Figure 7 : Nom de l'AC

Je laisse ensuite la période de validité à 5 année.

Et j'indique les emplacements de la base de données de certificats ainsi que le journal de la base.

		WINEVIL MELINELIOUN
i	Spécifier les emplacements des bases de donné	ées
2	Emplacement de la base de données de certificats :	
Č.	C:\Windows\system32\CertLog	
	Emplacement du journal de la base de données de certificats :	
	C:\Windows\system32\CertLog	
i		
	En savoir plus sur la base de données de l'autorité de certification	
	< Précédent Suivant >	Configurer Annuler

Figure 8 : Emplacement des bases de données

Il ne me reste plus qu'à faire Configurer pour finaliser la configuration. Mon Autorité de certification est maintenant configurer et fonctionnelle



Figure 9 : Autorité de certification fonctionnelle

#### b) Installation et configuration du Services de stratégie et d'accès réseau

Maintenant je vais procéder à l'installation du Services de stratégie et d'accès réseau qui corresponds au serveur NPS.

≧ <sup>v</sup>	Assistant Ajout de rôles et de fonctionnalités	
Sélectionner des	rôles de serveurs Sélectionnez un ou plusieurs rôles à installer sur le serveur sélect	SERVEUR DE DESTINATION WIN2012-M2LM2Llocal
Type d'installation	Rôles	Description
Selection du serveur Rôles de serveurs Fonctionnalités Services de stratégie et d' Services de rôle Confirmation Résultats	<ul> <li>Serveur DNS (Installé)</li> <li>Serveur Web (IIS)</li> <li>Services AD DS (Installé)</li> <li>Services AD FS (Active Directory Federation Servic</li> <li>Services AD LDS (Active Directory Lightweight Dire</li> <li>Services AD RMS (Active Directory Rights Manage</li> <li>Services d'activation en volume</li> <li>Services d'activation en volume</li> <li>Services d'impression et de numérisation de docu</li> <li>Services de certificats Active Directory (1 sur 6 inst</li> <li>Services de déploiement Windows</li> <li>Services de fichiers et de stockage (2 sur 12 install</li> <li>Services WSUS (Windows Server Update Services)</li> </ul>	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.
	< III >	
	< Précédent Suivant	> Installer Annuler

Figure 10 : Ajout des Services de stratégies d'accès réseau

Avant d'instaurer un nouveau client radius je vais réserver une adresse dans mon serveur DHCP, je vais la dédier à mon futur point d'accès Wifi.

	DHCP
Fichier Action Affichage ?	
Méservations	
<ul> <li>▲ invite win2012-m2l.t</li> <li>▲ invite invite</li></ul>	

Figure 11 : Réservation IP dans le serveur DHCP

J'ouvre maintenant mon serveur NPS pour passer à la configuration, pour ça je l'ouvre par le biais du Gestionnaire de serveur.



Figure 12 : Configuration 802.1X

Je choisis **Configurer 802.1X**, puis je sélectionne Connexions sans fil sécurisées et je renomme le type de connexion.

Configurer 802.1X				
Sélectionner le type de connexions 802.1X				
Type de connexions 802.1X :				
Onnexions sans fil sécurisées				
Lorsque vous déployez des points d'accès sans fil 802.1X sur votre réseau, le serveur NPS (Network Policy Server) peut authentifier et autoriser les demandes de connexion effectuées par les clients sans fil qui se connectent via ces points d'accès.				
○ Connexions câblées (Ethemet) sécurisées				
Lorsque vous déployez des commutateurs d'authentification 802.1X sur votre réseau, le serveur NPS (Network Policy Server) peut authentifier et autoriser les demandes de connexion effectuées par les clients Ethemet qui se connectent via ces commutateurs.				
Nom : Ce texte par défaut est utilisé pour composer le nom de chacune des stratégies créées à l'aide de cet Assistant. Vous pouvez vous servir du texte par défaut ou le modifier.				
WIFI-M2L				
Figure 13 : Connexions sans fil sécurisées				

Ensuite j'ajoute un nouveau client Radius qui est donc ma borne, je configure donc le Nom, l'adresse IP ainsi que le code secret partagé (ce code je devrais aussi le mettre dans la configuration de ma borne).

Propriétés de WIFI-M2L
aramètres
Sélectionner un modèle existant :
Nom et adresse
Nom convivial :
WIFI-M2L
Adresse (IP ou DNS) :
172.16.0.3 Vénfier
Sélectionnez un modèle de secrets partagés existant :
Aucun 🗸
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 Appliquer

*Figure 14 : Ajout d'un client Radius* 

Ensuite je choisis le type de protocole **EAP** pour cette stratégie, je sélectionne Microsoft : **PEAP**, et je le configure avec mon nouveau certificat.

J'ai besoin d'un mécanisme d'authentification de l'utilisateur qui souhaite se connecter au réseau. EAP (ou plus précisément Protected EAP) est le protocole idéal dans notre cas : il permet au point d'accès d'interroger un serveur d'identification (Radius) avant d'autoriser l'utilisateur à accéder aux ressources réseau de l'entreprise. Le serveur Radius, lui se chargera d'interroger l'Active Directory pour savoir si les informations d'authentification (login + password) sont valides ou pas : si oui, le serveur Radius donnera conformation au Point d'accès Wifi. La version de PEAP utilisée fait appel à un mécanisme d'authentification **MSCHAPv2** : le nom réel de la solution sera donc PEAP-EAP-MSCHAPv2 où l'authentification est faite par login/password. PEAP-EAP-TLS fait référence à un mécanisme d'authentification renforcé basé sur des certificats. (D'où l'installation d'un nouveau certificat).

	Configurer 802.1X	x
	Configurer une méthode d'authentification	
•	Sélectionnez le type de protocole EAP pour cette stratégie. Type (basé sur la méthode d'accès et la configuration réseau) :	
9	Microsoft: PEAP (Protected EAP)	



Modi	fier les propriétés EAP Proté	gé 🗙
Sélectionnez le certificat	que le serveur doit utiliser comme preu	ive de son
stratégie de demande de	connexion remplacera ce certificat.	ege dans la
Certificat délivré à :	M2L-WIN2012-M2L-CA	~
Nom convivial :	M2L-WIN2012-M2L-CA	
Émetteur :	M2L-WIN2012-M2L-CA	
Date d'expiration :	06/03/2021 17:40:39	
Activer la reconnexion	n rapide	
Deconnecter les client Types EAP	s sans chiffrement force	
Mot de passe sécurisé (E	AP-MSCHAP version 2)	Monter
		Descendre
Ajouter Modi	fier Supprimer OK	Annuler

Figure 16 : Sélection du certificat

Maintenant je spécifie le groupe d'utilisateurs qui aura accès à cette stratégie, ce groupe d'utilisateurs je l'ai au préalablement crée dans mon AD.

	Configurer 802.1X	X
	Spécifier des groupes d'utilisateurs	
	L'accès des utilisateurs membres du ou des groupes sélectionnés sera autorisé ou n fonction du paramètre d'autorisation d'accès de la stratégie réseau.	on en
Pour sélectionn stratégie s'appli	er des groupes d'utilisateurs, cliquez sur Ajouter. Si aucun groupe n'est sélectionné, cette ique à tous les utilisateurs.	
M2L\Uti-WIFI	Ajoute	er
	Suppri	mer



La configuration du nouveau client Radius est fini ainsi que sa stratégie d'accès. Mais il ne faut pas oublier d'inscrire le serveur dans l'AD.

<b>\$</b>	Serveur N	IPS (	Network Policy
Fichier Act	ion Affichage ?		
🚯 NPS (Laca	NPS (Locol)		
🔺 📔 Cli	Importer la configuration		
	Exporter la configuration		
⊿ jj Str.	Démarrer le service NPS Arrêter le service NPS Inscrire un serveur dans Active Directory		c Policy Server) vous tion des stratégies d' risation des demande
⊿ <b>№</b> Prc ▷ ₩	Propriétés Affichage	•	nfiguration dans la li
🗒 📲 Gesav	Aide		P)
👂 🌉 Gestio	n des modèles Protection d'accès	rése	au (NAP)
-	Figure 18 : Inscription d'un serveur dar	ns l'A	1D

 Serveur NPS (Network Policy Server)
 X

 Cet ordinateur est désormais autorisé à lire les propriétés de numérotation des utilisateurs du domaine M2L.local.
 Pour autoriser cet ordinateur à lire les propriétés de numérotation des utilisateurs d'autres domaines, vous devez l'inscrire en tant que membre du groupe de serveurs RAS/NPS dans les domaines concernés.

 OK

Figure 19 : Inscription du serveur dans l'AD

Afin d'avoir un suivi des tentatives de connexions, je configure le serveur pour qu'il me génère un fichier texte. Pour ça il faut aller dans « **Gestion** », et cliquer sur « **Configurer la gestion des comptes** ».



Je sélectionne donc « Enregistrer les données dans un fichier texte sur l'ordinateur local. »

Assistant Configuration de la gestion des comptes
Sélectionner les options de gestion
NPS peut enregistrer les données de gestion des comptes dans un fichier texte local, une base de données SQL Server uniquement, puis commencer à enregistrer dans un fichier texte si l'enregistrement SQL Server échoue, en fournissant le basculement.         Sélectionnez une option de configuration de la gestion des comptes NPS, et cliquez sur Suivant :         O Enregistrer les données dans un fichier texte su l'ordinateur local.         Image: Enregistrer les données dans un fichier texte su l'ordinateur local.         O Enregistrer les données dans un fichier texte sur l'ordinateur local.         O Enregistrer simultanément les données dans une base de données SQL Server et dans un fichier texte local.         O Enregistrer les données dans un fichier texte sur l'ordinateur local.         O Enregistrer les données dans un fichier texte sur l'ordinateur local.         O Enregistrer dans une base de données SQL Server et dans un fichier texte local.         O Enregistrer dans une base de données SQL Server et dans un fichier texte pour le basculement.
Précédent Suivant Terminer Annuler

Figure 21 : Enregistrement des données sur le PC

Maintenant il me faut tout cocher afin d'après des fichiers Logs lisible et je choisis le chemin où je veux le créer.

Assistant Configuration de la gestion des comptes	×
Configurer la journalisation dans un fichier local	
Informations de journalisation : Sélectionnez les informations qui seront enregistrées dans le fichier texte configuré. Demandes de comptes Demandes d'authentification Statut régulier des comptes Statut régulier des authentifications Répertoire des fichiers journaux : Spécifiez un emplacement pour votre fichier journal. NPS crée le fichier avec un nom de fichier au format Inyymm.log. C:\Users\Administrateur\Desktop Action en cas d'échec de la journalisation : Si la journalisation échoue en raison de problèmes réseau ou autres, NPS peut continuer à traiter les demandes de connexion ou les ignorer afin de préserver la précision des données de gestion des comptes. Si NPS ignore les demandes de connexion, les utilisateurs n'ont pas accès au réseau via les clients RADIUS. Parcouris Independent de problèmes réseau ou autres. Si NPS ignore les demandes de connexion si la journalisation échoue.	
Précédent Suivant Terminer Annuler	

Figure 22 : Journalisation dans un fichier local

c) Configuration des propriétés des utilisateurs de l'Active Directory

Ensuite pour chaque utilisateur dont je veux donner l'accès au Wifi, il faut que je modifie quelques paramètres dans les propriétés comme :

Dans l'onglet Appel entrant, il faut Autoriser l'accès réseau.

	I	Propriét	és de : L	ionel Baptis	te	? X
Environnement	Sessions	Contrôle à	à distance	Profil des servio	es Bureau à dis	tance COM+
Autorisation d'a	accès résea	au	relephon		T Membre de	
Autoriser l'a	iccès					
C Refuser l'ac	ccès	_				
C Contrôler l'a	accès via la	Stratégie (	d'accès à d	istance		

Figure 23 : Appel entrant

L'ajouter au groupe Uti-WIFI.

	Propriétés de : Lionel Baptiste ? ×
Environnement Ses Général Adresse Membre de :	ssions Contrôle à distance Profil des services Bureau à distance COM+ Compte Profil Téléphones Organisation Membre de Appel entrant
Nom Utilisateurs du do. Uti-WIFI	Dossier Services de domaine Active Directory M2L.local/Users M2L.local/Utilisateurs M2L
	Figure 24 : Ajout dans le groupe Uti-WIFI

d) Mise en place d'une stratégie de groupe

Afin que les utilisateurs de la Maison des Ligues n'est pas besoin de configurer ses paramètres Wifi, je décide de créer une GPO afin que la configuration soit automatique à l'ouverture de leur session.

Pour ça j'ouvre la console de Gestion de stratégie de groupe et je crée un nouvel objet GPO que je renomme Stratégie WIFI 802.1X.

E.	Gestion de stratégie de groupe		_ <b>D</b> X
📓 Fichier Action Affichage Fenêtre ?			_ 8 ×
🗢 🔿 📶 💽 🚺			
Gestion de stratégie de groupe ⊿ A Forêt : M2L.local	Objets de stratégie de groupe dans M Contenu Délégation	/I2L.local	
⊿ 🙀 Domaines ⊿ 🏥 M2L.local	Nom État GPO	Filtre WMI	Modifié le
Default Domain Policy     Domain Contr     Difference Million	Nouvel objet GPO	Aucun(e)	20/10/2015 20/10/2015 05/12/2015
Mappage Stratégie WIFI	802.1X	ucun(e) ucun(e)	29/10/2015 29/10/2015 07/12/2015
▷ BAT-A ▷ BAT-B ○ BAT-B ○ BAT-C ○ BAT-C	PO source :	ucun(e) ucun(e)	07/12/2018 07/12/2018 07/12/2018
▷ SAT C (aucun) ▷ SAT D ▷ SAT C	OK Annuler	✓ ucun(e) ucun(e)	07/12/2015 08/12/2015
<ul> <li>Constant</li> <li>Constant&lt;</li></ul>			

*Figure 25 : Stratégie de groupe* 

Je fais bouton droit de la souris sur « **Stratégie WIFI 802.1X** », je clique sur le bouton droit « **Modifier** » et je développe « **Configuration ordinateur** »  $\rightarrow$  « **Stratégies** »  $\rightarrow$  « **Paramètres Windows** »  $\rightarrow$  « **Paramètres de sécurité** »  $\rightarrow$  Clique sur « **Stratégies de réseau sans fil** (IEEE802.11) »  $\rightarrow$  « **Créer une stratégie de réseau sans fil pour Windows Vista et versions ultérieures** »

Щ.	Éditeur de gestion des s	tratégies de groupe
Fichier Action Affichage ?		
🗢 🄿 🙍 🗔 🗔 🖄		
Nonfiguration ordinateur	Nom	Description
⊿ 🚞 Stratégies —	引 Stratégies de comptes	Stratégies de mot de passe et de verrouillage d
Paramètres du logiciel	📓 Stratégies locales	Stratégies des options d'audit, de droits d'utilis
⊿ Paramètres Windows	🧃 Journal des événements	Journal des événements
Stratégie de résolution de r	Groupes restreints	Groupes restreints
Scripts (démarrage/arrêt)	📑 Services système	Paramètres du service système
A Paramétres de sécurité	📑 Registre	Paramètres de sécurité du Registre
Strategies de comptes	🙀 Système de fichiers	Paramètres de sécurité du système de fichiers
Strategies locales	📗 🥡 Stratégies de réseau filaire (	IEEE 802.3) Administration de la stratégie de réseau câblé
Groupes restreints	📔 🎬 Pare-feu Windows avec for	nctions avancé Pare-feu Windows avec fonctions avancées de
Services système	📔 🚞 Stratégies du gestionnaire c	de listes de rés Stratégies de groupes relatives au nom, à l'icôn
> Registre	Stratégies de réseau sans fil	(IEEE 802.11) Administration de la stratégie de réseau sans fil
Svstème de fichiers	📫 Stratégies de clé pub	Créer une stratégie de réseau sans fil pour Windows Vista et versions ultérieures
Stratégies de réseau fila	📫 Stratégies de restrict	Créer une stratégie Windows XP
Pare-feu Windows avec	Protection d'accès re	A -tu-line
📔 Stratégies du gestionna	📔 Stratégies de contrôl	Actualiser
Stratégies de réseau sar	Stratégies de sécurite	Aide
Stratégies de clé publiq	Configuration avancée de l	a stratégie d'a Configuration avancée de la stratégie d'audit
	Figure 26 : Strate	égie de réseau sans fil

Je crée dans un premier temps une stratégie pour les postes informatiques sous Windows vista et plus récent.

J'ajoute donc un nom à ce profil et je l'attribue à mon SSID.

Propriétés de : WIFI-M2I         Géléral       Autorisations réseau         Les paramètres définis dans cette stratégie s'applique interfaces sans fil des ordinateurs clients.         Nom de la stratégie :         WIFI-M2L         Degcription :         WIFI pour Win vista et +         ✓         Utiliser le service de configuration automatique de <u>Windows pour les clients</u> Se connecter aux réseaux dispos dans l'ordre des pro         Propriétés de : Nouveau         Connexion         Sécurité         Nom de profil :         WIFI-M2L         Nom(s) réseau (SSID) :         M2L-WIFI-Lio	eront à toutes les : réseau WLAN fils affichés ci-après : profil
GetXéral       Autorisations réseau         Les paramètres définis dans cette stratégie s'applique interfaces sans fil des ordinateurs clients.         Nom de la stratégie :         WIFI-M2L         Degcription :         WIFI pour Win vista et +         ✓         Utiliser le service de configuration automatique de <u>Windows pour les clients</u> Se connecter aux réseaux dispos dans l'ordre des pro         Propriétés de : Nouveau         Connexion         Sécurité         Nom de profil :         WIFI-M2L         Nom (s) réseau (SSID) :         M2L-WIFI-Lio	eront à toutes les : réseau WLAN fils affichés ci-après : profil
Les paramètres définis dans cette stratégie s'applique interfaces sans fil des ordinateurs clients. Nom de la stratégie : WIFI-M2L Degcription : WIFI pour Win vista et + ✓ Utiliser le service de configuration automatique de Windows pour les clients Se connecter aux réseaux dispos dans l'ordre des pro Propriétés de : Nouveau Connexion Sécurité   Nom de profil : WIFI-M2L Nom(s) réseau (SSID) : M2L-WIFI-Lio	eront à toutes les : réseau WLAN fils affichés ci-après : profil
Nom de la stratégie :         WIFI-M2L         Degcription :         WIFI pour Win vista et +         ✓         Utiliser le service de configuration automatique de Windows pour les clients         Se connecter aux réseaux dispos dans l'ordre des pro         Propriétés de : Nouveau         Connexion         Sécurité         Nom de profil :         WIFI-M2L         Nom(s) réseau (SSID) :         M2L-WIFI-Lio	réseau WLAN fils affichés ci-après : profil
WIFI-M2L         Degcription :         WIFI pour Win vista et +         ✓         Utiliser le service de configuration automatique de <u>Wi</u> ndows pour les clients         Se connecter aux réseaux dispos dans l'ordre des pro         Propriétés de : Nouveau         Connexion         Sécurité         Nom de profil :         WIFI-M2L         Nom(s) réseau (SSID) :         M2L-WIFI-Lio	réseau WLAN fils affichés ci-après : profil
Description : WIFI pour Win vista et + ✓ Utiliser le service de configuration automatique de <u>Wi</u> ndows pour les clients Se connecter aux réseaux dispos dans l'ordre des pro Propriétés de : Nouveau Connexion Sécurité   Nom de profil : WIFI-M2L Nom(s) réseau (SSID) : M2L-WIFI-Lio	réseau WLAN fils affichés ci-après : profil
WIFI pour Win vista et +         ✓         Utiliser le service de configuration automatique de <u>Windows pour les clients</u> Se connecter aux réseaux dispos dans l'ordre des pro         Propriétés de : Nouveau         Connexion         Sécurité         Nom de profil :         WIFI-M2L         Nom(s) réseau (SSID) :         M2L-WIFI-Lio	réseau WLAN fils affichés ci-après : profil
✓       Utiliser le service de configuration automatique de Windows pour les clients         Se connecter aux réseaux dispos dans l'ordre des pro         Propriétés de : Nouveau         Connexion         Sécurité         Nom de profil :         WIFI-M2L         Nom(s) réseau (SSID) :         M2L-WIFI-Lio	réseau WLAN fils affichés ci-après : profil
Se connecter aux réseaux dispos dans l'ordre des pro Propriétés de : Nouveau Connexion Sécurité Nom de profil : WIFI-M2L Nom(s) réseau (SSID) : M2L-WIFI-Lio	fils affichés ci-après : profil
Propriétés de : Nouveau Connexion Sécurité Nom de profil : WIFI-M2L Nom(s) réseau (SSID) : M2L-WIFI-Lio	profil
Connexion Sécurité Nom de profil : WIFI-M2L Nom (s) réseau (SSID) : M2L-WIFI-Lio	
WIFI-M2L Nom(s) réseau (SSID) : M2L-WIFI-Lio	
Nom(s) réseau (SSID) : M2L-WIFI-Lio	
M2L-WIFI-Lio	
M2L-WIFI-Lio	Aiouter
M2L-WIFI-Lio	
	Supprimer
Type de réseau : Basé sur un p	oint d'accès
✓ Se connecter automatiquement lorsque ce rése	
🗍 Se connecter à un réseau favori prioritaire si ce	au est à portée
Se connecter même s'il ne s'agit pas d'un résez	au est à portée la est possible

Figure 27 : Configuration de la stratégie de réseau sans fil

Ensuite je vais dans l'onglet Sécurité, pour initialiser l'Authentification « **WPA2-Entreprise** » et le chiffrement « **AES** », je sélectionne la méthode d'authentification précédemment choisie « **PEAP** » ainsi que le mode d'authentification « **Utilisateur ou ordinateur** »

Propriétés de : WIFI-M2L	x
Connexion Sécurité	
Sélectionner les méthodes de sécurité pour ce réseau         Authentification :       WPA2-Enterprise         Chiffrement :       AES	
Sélectionner une méthode d'authentification réseau : Microsoft: PEAP (Protected EAP)	
Authentification de l'utilisateur ou de l'ordinateur         Nbre max. d'échecs d'authentification :         Image: Mettre en mémoire cache les informations utilisateur pour les futures connexions à ce réseau	
Avancé	
OK Annuler	

Figure 28 : Sécurité de la stratégie

Maintenant dans l'onglet Autorisations réseau, je décoche toutes les cases sauf « Autoriser l'utilisateur à afficher les réseaux refusés » et « Autoriser tout le monde à créer tous les profils utilisateur ».

Propriétés de : WIFI-M2L							
Général Autorisations réseau							
Il n'est pas nécessaire d'ajouter les réseaux sans fil configurés comme réseaux favoris à la liste d'autorisations.							
Nom du réseau (SSID) Type de réseau Autorisation							
M2L-WIFI-Lio Infrastructure Autoriser							
Ajouter Supprimer							
Empêch <u>e</u> r toute connexion aux réseaux ad hoc							
Empêcher toute connexion aux réseaux à infrastructure							
✓ Autoriser l'utilisateur à afficher les réseaux refusés							
Autoriser tout le monde à créer tous les profils utilisateur							
☐ Utiliser seulement des pr <u>o</u> fils de stratégie de groupe pour les réseaux autorisés							
Paramètres de stratégie Windows 7 et versions ultérieures Ne pas autoriser les ré <u>s</u> eaux hébergés							
☐ Ne pas autoriser les informations d'identification de l'utilisateur partagées pour l'authentification réseau							
Activer la <u>p</u> ériode de blocage (minutes) : 20							
□ Ne pas autoriser les groupes Wi-Fi Direct							
OK Annuler <u>A</u> ppliquer							

Figure 29 : Autorisation de la stratégie

A présent je refais clique droit et je crée une stratégie Windows XP de la même manière que pour vista et plus récent.

Nego	Description		Туре		
WIFI-M2L	WIFI pour Win	vista et +	Vista and Later Releases		
		Créer une st	tratégie Windows XP		
		Actualiser			
		Exporter la l	iste		
		Affichage +			
		Réorganiser Aligner les i	les icônes cônes	۲	
		Aide			

Figure 30 : Création d'une stratégie Win XP

Voilà ma GPO finit d'être paramétrée.

Nom	Description	Туре
WIFI-M2L	WIFI pour Win XP	XP
WIFI-M2L	WIFI pour Win vista et +	Vista and Later Releases

Figure 31 : Les deux stratégies d'accès réseau

Je peux donc l'appliquer à tous les Utilisateurs M2L.



#### e) Configuration du point d'accès Wifi WRT54GL

Pour finaliser l'installation de mon Wifi d'entreprise, il ne me reste plus qu'à configurer mon AP.

Pour ça je me connecte à celle-ci par le biais d'un navigateur Web en tapant son adresse IP.

Je désactive tout type de connexion WAN, je change le nom du routeur en « **WIFI-M2L** » et j'ajoute aussi le nom de mon domaine qui est celui du contexte M2L et de mon précédent projet « **M2L.local** ».

re IP du routeu	ır Wifi :
172.16.0.3	Adresse réserver dans mon DHCP
255.255.0.0	
172.16.0.254	Adresse de passerelle de mon serveur (Interface Ipcop du
172.16.0.1	Adresse DNS de mon serveur M2L.local
	re IP du routeu 172.16.0.3 255.255.0.0 172.16.0.254 172.16.0.1

Enfin je paramètre le « Relay DHCP » afin que le routeur Wifi, demande à mon serveur DHCP de distribuer des adresses IP aux utilisateurs du Wifi.

Configuration WAN	
Type de connexion WAN	
Type de connexion	Désactivé 🗸
STP	O Activer
aramètres facultatifs	
Nom du routeur	WIFI-M2L
Nom d'hôte	
Nom de domaine	M2L.local
MTU	Auto 🗸 1500
Configuration réseau	
Adresse IP du routeur	
Adresse IP	172. 16. 0. 3
Masque de sous-réseau	255. 255. 0. 0
Passerelle	172. 16. 0. 254
DNS local	172, 16, 0, 1
Port WAN	
Ajouter le port WAN au Switch	
Paramètres du serveur d'adresse d	le réseau (DHCP)
Type de DHCP	Transfert de DHCP 🗸
Serveur DHCP	172, 16, 0, 1

Figure 33 : Configuration réseau + relay DHCP

A présent je configure le réseau Wifi de celui-ci, je choisis donc le SSID en fonction de celui que j'ai initialiser lors de la configuration de ma GPO, soit « M2L-WIFI-Lio ».

dd-wrt.cc	)m cor	ntrol p	banel		Heure: 05:37:1	18 up 5:37,	load aver	age: 0.05, 0.08, 0.08 WAN: Désactivé
Configuration Sans fil	Services Sécurit	é Restric	tions d'accès	NAT / Qo	S Adminis	stration	État	
Paramètres de base Radius	Sécurité sans fil F	Filtrage MAC	Paramètres ava	ancés W	DS			
Interface sans fil wl0						Aide		plus
Interface sails in wide       Mode         Interface sails in wide       Interface sails in wide         Interface sails in wide       Interface physique wide - SSID [M2L-WIFI-Lio] HWAddr [C0:C1:C0:59:B7:0A]       Mode sans fil         Mode sans fil       AP       v         Mode réseau sans fil       Mixte       v         Nom du réseau sans fil       Mixte       v         Nom du réseau sans fil       Mixte       v         Canal sans fil       Auto       v         Diffusion SSID sans fil       Image: Configuration réseau       Obésactiver         Sensibilité (ACK Timing)       2000       (Défaut: 2000 mètres)         Configuration réseau       Unbridged       Bridged							ns fil: a fois des 11 get 802.11b sur ervez le paramètre iphériques ez <i>G-uniquement</i> . iquement avec des 11b, sélectionnez 11b, sélectionn	
Interfaces virtuelles						Sensibili	té :	
	Ajou Enregistrer Ap	pliquer	Annuler			Permet de désactive fonctionna Broadcom chipset At ack timing	régler le complèter alité pour l . Pour ceu heros cela automatic	ack timing. 0 ment cette les Micrologiciels ix basés sur un a bascule en mode que

Figure 34 : Configuration WIFI de base

Ensuite je configure le serveur Radius « **Remote Authentification Dial-In User Service** ». Je l'active, j'insère l'adresse de mon serveur Radius qui est donc celle de mon serveur de domaine, j'attribue le port du serveur, qui est par défaut « **1812** ».

Je choisis le format du mot de passe qui est la clé partagée précédemment initialiser à la création du client radius sur le serveur NPS. Puis j'enregistre la configuration.

Configuration Sans fil	Services Sé	curité Restri	ctions d'accès	NAT	/ QoS	Adminis			
Paramètres de base Radiu	s Sécurité sans fil	Filtrage MAC	Paramètres av	ancés	WDS				
Remote Authenticatio	n Dial-In User Se	rvice (RADIUS	5)						
RADIUS									
Identification RADIUS	Active	O Désactiver							
Format adresse MAC	aa:bb:cc:c	d:ee:ff ∨							
Adresse du serveur RADIUS	172.	16.0.	1						
Port du serveur RADIUS	1812								
Utilisateurs non identifiés Max.	999								
Format du mot de passe	Clé par	tagée 🔿 Adress	e MAC						
Secret partagé RADIUS	•••••	••••	Afficher						
Outrepasser l'identification en	cas 🗌								
d'indisponibilité du serveur RAI	DIUS								
	Enregistrer	Appliquer	Annuler						

Figure 35 : Configuration Radius

Et pour finir je vais dans l'onglet « **Sécurité sans fil** », je sélectionne le mode de sécurité « **WPA2-Entreprise** », cryptage WPA « **AES** », l'adresse de mon serveur Radius, le port par défaut du serveur Radius et encore une fois la clé partagée. Puis j'enregistre.

dd-wrt.co	mc	cont	rol p	banel		Heu	re: 05:38:02
Configuration Sans fil	Services	sécurité	Restric	tions d'accès	NAT	/ Qo5	Administr
Paramètres de base Radius	Sécurité sans	fil Filtra	age MAC	Paramètres ava	ancés	WDS	
Sécurité sans fil wl0							
Interface physique wl0 SSID [I	M2L-WIFI-Lio] H	WAddr [C	0:C1:C0:59	9:B7:0A]			
Mode de Sécurité	WPA2 E	nterprise	¥				C
Cryptage WPA	AES	¥					d
Adresse du serveur RADIUS	172	. 16 .	0.	1			
Port du serveur RADIUS	1812	]		(Défaut: 181)	2)		
Secret partagé RADIUS	•••••	•••••		Aff	ficher		
Délai de renouvellement des dés secondes)	(en 3600						
	Enregi	strer	Appliquer				

Figure 36 : Configuration de la sécurité sans fil

#### 4. Conclusion

La situation professionnelle est basée sur le contexte de la Maison des Ligues de Lorraine, comme pour le précédent projet. D'ailleurs je me suis servi de mon premier projet pour effectuer celui-ci. Il m'a été demandé de créer un Wifi d'entreprise sécurisé, après l'étude de plusieurs solutions, j'ai opté pour sécuriser mon **Wifi**, d'utiliser un serveur **NPS** avec authentification **PEAP**. Cela me permet d'être dans la continuité de mon projet 1 car cette méthode d'authentification utilise les comptes utilisateurs de l'**Active directory** ainsi que le serveur **DHCP** et **DNS** de mon contrôleur de domaine. L'infrastructure réseau existante ne disposait pas de WIFI. J'ai donc mis en place un serveur de domaine «**M2L** » avec **Active Directory, DNS, DHCP et NPS**. J'ai utilisé une **GPO** pour automatiser les paramètres d'authentification sur le SSID **M2L-WIFI-Lio**. Grâce à cette GPO, l'utilisateur n'a rien à faire pour accéder au Wifi d'entreprise, la GPO fait le lien avec son login et password de l'AD afin d'authentifier l'utilisateur au serveur NPS.

Maintenant La Maison des Ligues dispose d'un accès internet sécurisé via un pare-feu ainsi d'un serveur de domaine disposant d'un Active Directory, DHCP, DNS, NPS et d'une connexion WIFI sécuriser au maximum. Chaque bâtiment dispose d'un répertoire dédié, ainsi qu'un répertoire commun.

Grâce à ce type d'authentification, les utilisateurs équipés de smartphone, pourront se connecter au réseau Wifi d'entreprise par le biais de leur identifiant/mot de passe de l'AD (celui qu'ils utilisent pour ouvrir l'un session).