

ACCESS POINT_RADIUS

Table des matières

Objectif(s) :	Error! Bookmark not defined.
Légende :	Error! Bookmark not defined.
1. Travail préparatoire :	4
2. Configuration :	4
3. Sécurisation minimale :	5
4. Sécurité et management :	7
5. Serveur Radius EAP-MD5 / EAP-LEAP :	11

Objectif :

L'objectif de cette procédure est de mettre en place un serveur RADIUS avec un point d'accès WIFI.

Prérequis :

- Access point
- RADIUS

Légende :

Les textes surlignés en jaune correspondent à des commandes ou à des indications qui permet de justifier les résultats obtenus ou de montrer des informations qu'elles doivent être respectées.

1. Travail préparatoire :

Il faut d'abord réinitialiser la borne wifi. Il faut donc mettre sous aucune alimentation la borne wifi et appuyer sur le bouton situé à l'arrière de la borne. Tout en restant appuyer sur le bouton, il faut reconnecter le câble d'alimentation. Dès que le voyant devient orange, relâcher le bouton et laisser la borne démarrer.

Il faut ensuite aller configurer l'interface web de la borne wifi, pour y avoir accès, il faut commencer par lui attribuer une adresse IP.

On se connecte alors avec le câble console + Putty

Mode console :

enable

Password : Cisco

conf t

Interface bvi1

ip address 192.168.1.X 255.255.255.0

no shutdown

exit

On peut ensuite accéder à l'interface web : http:192.168.1.11 *Adresse IP choisie dans notre exemple*

Pour ce se connecter à l'interface, utilisateur Cisco et mot de passe Cisco

2. Configuration :

Création du SSID et qu'il se diffuse

Mode console : (Hector correspond au nom de la borne wifi)

conf t

dot11 ssid HECTOR

authentication open

guest-mode

exit

interface dot11radio 0

ssid Hector

On vérifie ensuite que l'interface radio n'est pas down :

Mode console:

show ip interface brief

Si l'interface dot11radio 0 n'est pas up, pour corriger le problème, entrer les commande suivantes :

Mode console :

conf t

interface dot11radio 0

no shutdown

Il faut ensuite vérifier que l'authentification est ouvert.

Mode console :

conf t

dot11 ssid HECTOR

authentication exit

On va ensuite diffuser notre SSID « HECTOR »

Mode console :

dot11 ssid HECTOR

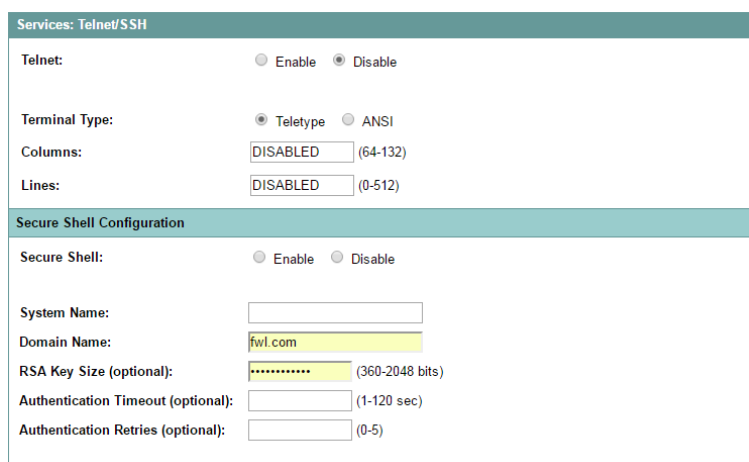
guest-mode

3. Sécurisation minimale :

Mise en place de l'accès SSH

Pour réaliser cela, il faut aller dans le menu SERVICES puis sélectionner l'onglet Telnet/SSH. Désactiver le telnet et activer SSH en modifiant éventuellement le nom de domaine et le nom du système.

Ne marche pas en réalité.



Services: Telnet/SSH	
Telnet:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Terminal Type:	<input checked="" type="radio"/> Teletype <input type="radio"/> ANSI
Columns:	DISABLED (64-132)
Lines:	DISABLED (0-512)

Secure Shell Configuration	
Secure Shell:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
System Name:	<input type="text"/>
Domain Name:	fwl.com
RSA Key Size (optional):	***** (360-2048 bits)
Authentication Timeout (optional):	<input type="text"/> (1-120 sec)
Authentication Retries (optional):	<input type="text"/> (0-5)

Mise en place d'une encryption

En l'occurrence il s'agit de définir une encryption WEP3. Pour cela, dans l'onglet Encryption Manager du menu SECURITY, régler votre clef WEP

	Transmit Key	Encryption Key (Hexadecimal)	Key Size
Encryption Key 1:	<input checked="" type="radio"/>	*****	40 bit
Encryption Key 2:	<input type="radio"/>		128 bit
Encryption Key 3:	<input type="radio"/>		128 bit
Encryption Key 4:	<input type="radio"/>		128 bit

Mise en place d'une authentification OPEN + MAC

Pour cela, dans l'onglet SSID Manager du menu SECURITY, choisissez l'option with MAC Authentication

Methods Accepted:

- Open Authentication: with MAC Authentication
- Shared Authentication: < NO ADDITION >
- Network EAP: < NO ADDITION >

Ensuite, dans l'onglet Advanced Security du menu SECURITY, entrer la liste local des adresses MAC qui seront autorisée à se connecter

Local MAC Address List

Local List: bc6c.21dd.b25c
fc3f.7ce4.9ce1

New MAC Address: (HHHH.HHHH.HHHH)

Mise en place d'un nouvel administrateur

Local User List (Individual Passwords)

User List:

< NEW >
Wifi_HML
Admin

Delete

Username:

Password:

Confirm Password:

Capability Settings: Read-Only Read-Write

4. Sécurité et management :

- Désactiver la diffusion du SSID :

Pour désactiver la diffusion du SSID il suffit d'aller dans l'onglet SECURITY puis dans SSID Manager :

Guest Mode/Infrastructure SSID Settings

Set Beacon Mode: Single BSSID **Set Single Guest Mode SSID: < NONE >** Multiple BSSID

Set Infrastructure SSID: Force Infrastructure Devices to associate only to this SSID

Apply Cancel

Il faut placer le « SET SINGLE GUEST MODE SSID » en NONE afin que le SSID ne se diffuse plus.

- Filtrage par adresse MAC :

Tout d'abord il faut sélectionner l'option « With MAC Authentication » dans l'onglet SSID Manager :

Current SSID List

< NEW >
HECTOR

SSID: HECTOR
VLAN: < NONE > Define VLANs
Backup 1:
Backup 2:
Backup 3:
Interface: Radio0-802.11G
Network ID: (0-4096)

Delete

Client Authentication Settings

Methods Accepted:

Open Authentication: with MAC Authentication

Puis dans l'onglet Advanced security:

Il suffit ensuite simplement de rentrer les adresses macs que l'on souhaite.

Local MAC Address List

Local List:

bc6c.21dd.b25c
fc3f.7ce4.9ce1

Delete

- Changement du chiffrement par clef WEP par un chiffrement fort de type Cipher (WEP + TKIP, TKIP ou autre) ;

Pour changer de chiffrement, il faut se diriger vers l'onglet « Encryption Manager »

Puis sélectionner Cipher, et nous allons mettre TKIP + WEP 40 Bits :

Security: Encryption Manager

Encryption Modes

None

WEP Encryption Optional

Cisco Compliant TKIP Features: Enable Message Integrity Check (MIC)
 Enable Per Packet Keying (PPK)

Cipher TKIP + WEP 40 bit

- Création d'un utilisateur nommé Wifi_HML (Hirbec, Mariette, Letort)

Pour faire ceci il suffit d'aller dans l'onglet Advanced Security :

Local User List (Individual Passwords)

User List:

< NEW >
Cisco

Delete

Username: Wifi_HML

Password:

Confirm Password:

Capability Settings: Read-Only Read-Write

Apply Cancel

Mot de passe de l'utilisateur : testwifi0

Résultat :

< NEW >
Cisco
Wifi_HML

- Supprimer l'utilisateur Cisco et configuration d'un compte administrateur

Ceci se trouve dans le même onglet, Nous allons mettre comme login et mot de passe « Admin »

Local User List (Individual Passwords)

User List:

< NEW >
Cisco
Wifi_HML

Delete

Username: Admin

Password:

Confirm Password:

Capability Settings: Read-Only Read-Write

Apply Cancel

Local User List (Individual Pas

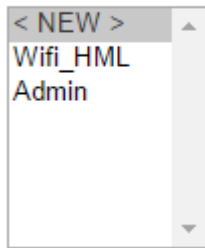
User List:

< NEW >
Cisco
Wifi_HML
Admin

Delete

Pour supprimer l'utilisateur il suffit ensuite de faire DELETE

User List:



A dropdown menu with a scroll bar. The items listed are: < NEW >, Wifi_HML, and Admin.

- Désactivation des services inutiles, et activation du SSH :

Nous allons ici désactiver le Telnet et mettre en place le SSH,

Pour cela allons dans l'onglet SERVICES, puis dans Telnet/SSH.

Services: Telnet/SSH

Telnet: Enable Disable

Secure Shell Configuration

Secure Shell: Enable Disable

System Name:
Domain Name:
RSA Key Size (optional): (360-2048 bits)
Authentication Timeout (optional): (1-120 sec)
Authentication Retries (optional): (0-5)

Cf 5.SECURISATION MINIMALE afin de voir comment configurer le SSH.

- Création d'une liste d'accès interdisant votre PC sans fil de faire une requête http sur le PC fixe.

5. Serveur Radius EAP-MD5 / EAP-LEAP :

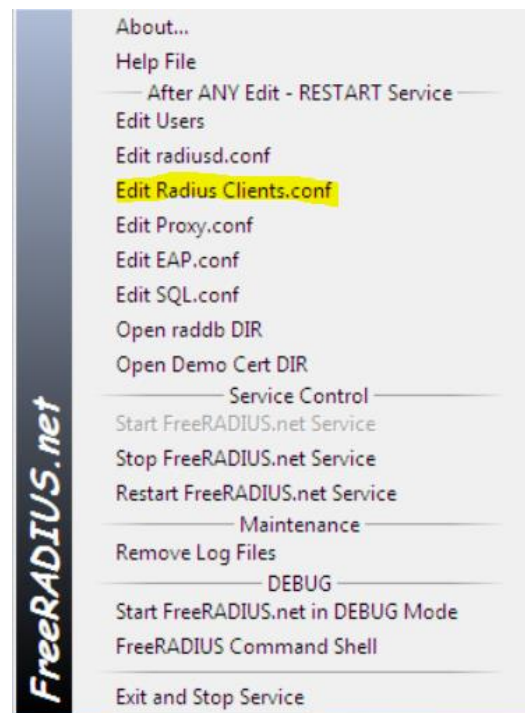
EAP-MD5 est un autre standard ouvert IETF, mais il offre un niveau de sécurité faible. La fonction de hachage MD5 utilisée est vulnérable aux attaques par dictionnaire, et elle ne supporte pas clef WEP dynamiques.

Lightweight Extensible Authentication Protocol (LEAP) est une implémentation propriétaire d'EAP conçue par Cisco. Ce protocole n'est pas présent nativement sous Windows. Il était connu pour être vulnérable aux attaques par dictionnaire comme EAP-MDP5. Mais il ne l'est plus depuis la version de 2003. Cisco continue de soutenir que LEAP est une solution sécurisée si l'on utilise des mots de passe suffisamment complexes.

Pour installer le serveur RADIUS, on crée un partage réseau pour récupérer le setup afin de le lancer sur une machine virtuelle.

Afin de configurer le serveur RADIUS, on édite le fichier clients.conf afin d'indiquer qui sera le client du serveur :

```
client 192.168.1.11/24 {  
    secret      = root  
    shortname   = MHL10  
    nastype    = cisco  
}
```



On édite ensuite le fichier Users afin d'indiquer qui sera en mesure de se connecter et on rajoute les lignes suivantes :

```
adminloc  
Auth-Type := EAP, User-Password == "cna-tp"  
Reply-Message = "Authentification réussie"
```

On fait un clic droit sur l'icône du serveur RADIUS et on clique sur START FreeRadius.net in DEBUG MODE. Une fenêtre s'ouvre et effectue des requêtes si tout c'est bien passer

Configuration de l'authenticator :

Après avoir attribué BV11 du point d'accès l'adresse 192.168.1.11/24, utilisez l'interface graphique pour configurer l'authenticator. Cette configuration se fait dans le menu SECURITY.

Tout d'abord, cliquez sur SSID manager afin de définir un SSID et de sélectionnez l'utilisation du protocole EAP comme transport de la méthode d'authentification. Un message vous demandant de définir une encryptions apparaîtra, cliquez sur OK et continuer.

Security: Global SSID Manager

SSID Properties

Current SSID List

< NEW >
HECTOR

SSID: HECTOR

VLAN: < NONE > [Define VLANs](#)

Backup 1:
Backup 2:
Backup 3:

Interface: Radio0-802.11G

Network ID: (0-4096)

Delete

Client Authentication Settings

Methods Accepted:

Open Authentication: with EAP

Shared Authentication: < NO ADDITION >

Network EAP: < NO ADDITION >

Ensuite, cliquez sur encryption Manager afin de définir une clef WEP (ou autre toute autre encryption que le client supporte)

Security: Encryption Manager

Encryption Modes

None

WEP Encryption [Mandatory](#)

Cipher [TKIP + WEP 40 bit](#)

Cisco Compliant TKIP Features: Enable Message Integrity Check (MIC)
 Enable Per Packet Keying (PPK)

Encryption Keys

Encryption Key 1: Transmit Key Encryption Key (Hexadecimal)

Key Size: 40 bit

Enfin, cliquez sur le Server Manager afin d'indiquer au point d'accès :

1. L'adresse IP du serveur radius
2. Le secret partagé correspond a root ajouter précédemment
3. Les ports utilisés

Corporate Servers

Current Server List

RADIUS

< NEW >

Delete

Server: 192.168.1.136 (Hostname or IP Address)

Shared Secret:

Authentication Port (optional): 1812 (0-65536)

Accounting Port (optional): 1813 (0-65536)

N'oubliez pas également de fixer le Default Server Priorities avec l'adresse IP du serveur radius.

Default Server Priorities

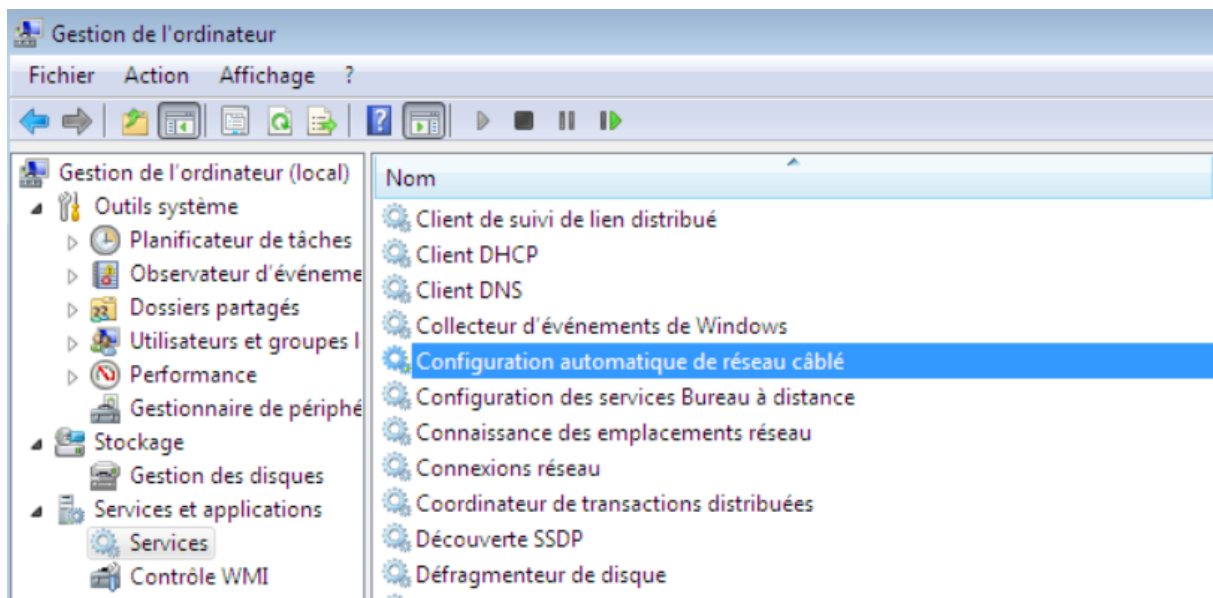
EAP Authentication

Priority 1: 192.168.1.136

Configuration du supplicant :

Vous devez juste configurer un profil pour lequel dans l'onglet Security vous aurez sélectionné la méthode le 802.1X, choisi une authentification de type LEAP, et configuré la demande d'un login et d'un password.

Sur le serveur RADIUS, on fait un clic droit sur ordinateur dans le menu démarrer. Ensuite, on démarre le service Configuration automatique de réseau câblé :



Ensuite, on fait un clic droit pour afficher les propriétés de la carte réseau. On va dans l'onglet Authentification, on choisit Microsoft PEAP et dans Paramètres Supplémentaires, on coche sur Spécifier le mode d'authentification.

