# **TUTORIEL RADIUS**

Dans ce tutoriel nous allons voir, comment mettre en place une borne wifi avec un protocole RADIUS. Pour cela, vous aurez besoin : - d'un serveur Windows 2012

- d'un Active Directory

- d'une borne wifi (D-Link dans notre cas).

# I. Qu'est-ce que RADIUS ?

RADIUS (Remote Authentication Dial-In User Service) est un protocole client-serveur permettant de centraliser des données d'authentification. Le protocole RADIUS permet de faire la liaison entre des besoins d'identification et une base d'utilisateurs en assurant le transport des données d'authentification de façon normalisée.

L'opération d'authentification est initiée par un client du service RADIUS, qui peut être un boîtier d'accès distant (NAS : Network Access Server), un point d'accès réseau sans fil, un pare-feu (firewall), un commutateur, un autre serveur. Le serveur la traite en accédant si nécessaire à une base externe : base de données SQL, annuaire LDAP, comptes d'utilisateur de machine ou de domaine ; un serveur Radius dispose pour cela d'un certain nombre d'interfaces ou méthodes.

### II. Création d'un groupe et d'utilisateur

Pour commencer il faut crée un groupe de travail dans l'active directory et un utilisateur. Lorsque l'utilisateur est crée il faut faire un clic droit, propriété sur l'utilisateur et accorder l'accès au réseau, de cette façon :

Général Adres	Sessions Contrôle à distance Profil des s se Compte Profil Téléphones Organis	ervices Bureau à distance COM- sation Membre de Appel entran
- Autorisation of Autoriser I Refuser I Contrôler	l'accès réseau 'accès accès 'accès via la Stratégie d'accès à distance	
Options de ra	lentité de l'appelant : ppel	
C Défini pa	rl'appelant (service de routage et d'accès à dis rappeler :	stance uniquement)
C Défini pa C Toujours - Attribuer d Définissez le d'appel entr	rl'appelant (service de routage et d'accès à dis rappeler : les adresses IP statiques es adresses IP à activer pour cette connexion ant.	stance uniquement) Adresses IP statiques

### III. Mise en place du serveur RADIUS

Network Policy Server (NPS) peut être utilisé comme serveur RADIUS afin d'effectuer l'authentification, l'autorisation et la gestion des clients RADIUS.

NPS utilise un domaine AD DS pour l'authentification des informations d'identification utilisateur des messages de demande d'accès RADIUS entrants.

Il est nécessaire d'installer le rôle IIS afin d'obtenir un certificat pour que le serveur puisse répondre au requête RADIUS, nous allons donc installer le rôle Services de Stratégie d'Accès Réseau et IIS.

Dans « Gérer » choisissez « Ajouter des rôles et fonctionnalité » et sélectionnez les rôles correspondant :

Sélectionner des	s rôles de serveurs	SERVEUR DE DESTINATIO srv15.Domaine11.ne
Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs	Rôles	Description L'accès à distance offre une connectivité transparente, toujours
Fonctionnalités Confirmation Résultats	Services AD DS (Installé)     Services AD DS (Installé)     Services AD DS (Active Directory Federation Service     Services AD LDS (Active Directory Lightweight Dire     Services AD RMS (Active Directory Rights Manage     Services Bureau à distance     Services d'activation en volume     Services d'activation en volume     Services de certificats Active Directory     Services de déploiement Windows     Services de stratégie et d'accès réseau     Services WSUS (Windows Server Update Services)	active et toujours gérée basée sur DirectAccess. L'accès à distance fournit des services VPN traditionnels, y compris la connectivité de site à site (succursa ou nuage). Le routage fournit des fonctionnalités de routage traditionnelles, y compris la traduction d'adresses réseau et d'autres options de connectivité.
	< III >	

Pour les services de Rôle IIS laissez tous par défaut, du moins pour la présentation actuel, si vous avez besoin d'autres services sélectionnez les, le certificat dans le rôle IIS est intégré de base, c'est une fonctionnalité obligatoire. Pour le NPS sélectionnez « Serveur NPS»

1	Serveur NPS (Network Policy Server)
-	Services Routage et accès distant
	Service d'accès à distance
	Routage
	Autorité HRA (Health Registration Authority)
	HCAP (Host Credential Authorization Protocol)

Maintenant que le serveur NPS est installé, rendez-vous sur l'interface de ce serveur et joignez-le à l'Active Directory :



Erduan HOXHA 3 Crée un nouveau client RADIUS et saisir les informations nécessaires : nom convivial, adresse IP du serveur et le secret partagé :

🚯 NPS (Local)	Cli	ents RADIUS	
🔺 🛄 Clients et ser	veurs RADIUS		
Client-P	Nouveau	au.	4
Group	Nouveau		
Strategies	Exporter la liste	al Adre	s
Gestion	Affichage	•	
▷ Image: Section d	Actualiser		
	Aide		
	1		
	1		
Nouv	eau client RAI	אוור	X
NOUV	cau chent iva	0105	
Paramètres Avancé			
Avalice			î
Activer ce client RADIUS			
Sélectionner un modèle existant	· ·		
			~
Nom et adresse			
Nom convivial :			
raduis-wifi			
Adresse (IP ou DNS) :			
192.168.0.218		1	/érifier
Secret nartagé			
Sélectionnez un modèle de secre	ts partagés existant	<u>,</u>	
Augun	ta partagea existant	···	
Aucun			¥
Pour taper manuellement un secre	et partagé, cliquez s	sur Manuel, Pour gér	nérer
client BADIUS avec le même sec	ge, cliquez sur Gen ret partagé entré ic	erer. Vous devez con Les secrets partag	ntigurer le
respectent la casse.	iot partage critic to	. Los sociolo partag	
Manuel     Gé	nérer		
Secret partagé			
Confirmaz la scoret podocá :			
commezie secret partage :			
		-	
		OK	Annuler

Puis valider en cliquant sur OK.

Ensuite, vous devez crée une stratégie de demande de connexion :



Donnez un nom à la stratégie (« wifi » dans notre cas) :

Vous devez rajouter des conditions : - le nom d'utilisateur (Erduan dans notre cas) - le type de port (sans fil)

HCAP		1
	Groupes d'emplacements La condition Groupes d'emplacements HCAP spécifie les groupes d'emplacements HCAP (Host Credential Authorization Protocol) nécessaires pour correspondre à cette stratégie. Le protocole HCAP sert à la communication entre le serveur NPS et des serveurs NAS tiers. Consultez la documentation de votre serveur NAS avant d'utiliser cette condition.	ш
Nom d	'utilisateur	
88.	Nom d'utilisateur Nom d'utilisateur employé par le client d'accès à distance dans le message RADIUS. Cet attribut est une chaîne de caractères qui contient généralement un nom de domaine et un nom de compte d'utilisateur.	
Propri	etes de la connexion	
ļ	Adresse IPv4 du client d'accès La condition d'adresse IPv4 du client d'accès spécifie l'adresse IPv4 du client d'accès qui demande l'accès à partir	

Veuillez cocher ces cases pour le type de port NAS :

Type de port	NAS
Spécifiez les types de médias d'accès nécessaires Types de tunnels pour connexions d'accès à dista	pour correspondre à cette stratégie. nce et VPN standard
Asynchrone (Modem) RNIS synchrone Synchrone (ligne T1) Virtuel (VPN)	
Types de tunnels pour connexions 802.1X standar  Ethemet FDDI	d
Sans fil - IEEE 802.11	
Autres RNIS asynchrone V.120 RNIS synchrone Sans fil - Autre	^
SUSL - USL symetrique	
	Annuler

Puis laisser les autres paramètres par défaut et « Suivant ».

Il faut à présent crée une stratégie de réseau possédant le même nom que la stratégie précédemment crée (« wifi » dans notre cas) et rajouter les conditions suivantes :

- les groupes d'utilisateurs (bts dans notre cas)

- le type de port (avec les mêmes types de port qu'au dessus)

Group	es de la companya de	1
<b>1</b>	Groupes Windows La condition Groupes Windows spécifie que l'utilisateur ou l'ordinateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.	
	Groupes d'ordinateurs La condition Groupes d'ordinateurs spécifie que l'ordinateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.	
	Groupes d'utilisateurs La condition Groupes d'utilisateurs spécifie que l'utilisateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.	
	Groupes d'emplacements La condition Groupes d'emplacements HCAP spécifie les groupes d'emplacements HCAP (Host Credential Authorization Protocol) nécessaires pour correspondre à cette stratégie. Le protocole HCAP sert à la communication estre la consume NPS et des courses NAS fines. Consultant la desurse tratégies de surse avec NAS estre d'étilises	

Puis, il faut bien évidement accordé l'accès :



Concernant les méthodes d'authentification, il faut ajouter le protocole EAP et cocher les cases suivantes :

a demande de connexion ne repon ntraintes :	pas a toutes les contraintes, l'acces reseau est refuse.	
Contraintes Méthodes d'authentification Délai d'inactivité	Autorisez l'accès uniquement aux clients qui s'authentifier spécifiées. Les types de protocoles EAP sont négociés entre le serve l'ordre dans lequel ils sont listés.	nt à l'aide des méthodes eur NPS et le client dans
<ul> <li>session</li> <li>ID de la station appelée</li> <li>Restrictions relatives aux jours et aux heures</li> <li>Type de port NAS</li> </ul>	Microsoft: PEAP (Protected EAP)          III         Ajouter       Modifier         Supprimer         Méthodes d'authentification moins sécurisées :         Authentification chiffrée Microsoft version 2 (MS-CHAP)         I L'utilisateur peut modifier le mot de passe après sor         Authentification chiffrée Microsoft (MS-CHAP)         III         III         Méthodes d'authentification chiffrée Microsoft version 2 (MS-CHAP)         Authentification chiffrée Microsoft (MS-CHAP)         I L'utilisateur peut modifier le mot de passe après sor         Authentification chiffrée (CHAP)         Authentification non chiffrée (PAP, SPAP)         Autoriser les clients à se connecter sans négocier une         Vérifier uniquement l'intégrité de l'ordinateur	Monter Descendre

Vous devez laisser les paramètres suivants par défaut, et valider la stratégie.

# IV. Configuration de la borne wifi

Maintenant que le serveur RADIUS est configuré sur le Windows SERVER 2012, il est nécessaire de configurer la borne wifi. Ouvrez votre navigateur et entré l'adresse IP de la borne (dans notre l'adresse IP par défaut est 192.168.0.50). Vous devez vous rendre dans le menu du LAN à gauche et modifier l'IP de la borne :

Hom	ne Ad	vanced	Tools		Status	Help
LAN Setti	ings	1	Statia (Manual)	820	1	
IP Addres	s		192.168.0.219			
Subnet M	lask		255.255.255.0			
Default Ga	ateway	1	192.168.0.1		255	

Puis, vous devez aller dans le menu Wireless à gauche et modifier les informations de façon à obtenir ce type de configuration :

- Authentification: WP2-EAP
- RADIUS Server : l'adresse IP du serveur (192.168.0.161 dans notre cas)
- RADIUS Port : port par défaut (1812)
- RADIUS Secret : le secret partagé crée dans le serveur NPS

	Propriétés de : erdua	n	? X
Environnement Sessior Général Adresse Con	ns Contrôle à distance Profil des s npte Profil Téléphones Organis	ervices Bureau à dista sation Membre de	ance COM+ Appel entrant
Autorisation d'accès ré     Autoriser l'accès     Refuser l'accès     Contrôler l'accès vi	iseau a la Stratégie d'accès à distance		
Vérifier l'identité de     Options de rappel     Pas de rappel     Défini par l'appelar     Toujours rappeler	l'appelant :	stance uniquement)	
<ul> <li>Attribuer des adress</li> <li>Définissez les adresse</li> <li>d'appel entrant.</li> </ul>	ses IP statiques es IP à activer pour cette connexion	Adresses IP statiqu	ies
Appliquer les itinéra Définir les itinéraires à d'appel entrant.	ires statiques activer pour cette <mark>c</mark> onnexion	Itinéraires statiqu	es
	OK Annuler	Appliquer	Aide

#### V. Joindre le réseau WIFI

Pour pouvoir joindre le réseau wifi, il est nécessaire de faire quelques modifications. Allez dans Panneau de configuration, puis Réseau et Internet, Gérer les réseaux sans fil et cliquer sur Ajouter (pour ajouter un réseau sans fil) :



Puis Créer un profil réseau manuellement et entrez les informations nécessaires (nom réseau, type de sécurité, type de chiffrement et la clé de sécurité).

Entrer les information	ons relatives au réseau s	ans fil à ajouter
Nom réseau :	Erduan	
Type de sécurité :	WPA - Entreprise	•
Type de chiffrement :	AES	•
Clé de sécurité :		Masquer les caractères
📝 Lancer automatiqu	ement cette connexion	
🔲 Me connecter mêr	ne si le réseau ne diffuse pas so	n nom
Attention : si vous risque.	sélectionnez cette option, la sé	curité de votre ordinateur peut courir un

Lorsque les informations sont entrées, il est nécessaire de modifier les paramètres de connexion :

ropriétés du réseau s	sans fil Radius_Wifi	Propriétés du réseau sans fil Radius_Wifi	83
Connexion Sécurité		Connexion Sécurité	
Nom : SSID : Type de réseau : Disponibilité du réseau :	Erduan Erduan Point d'accès Tous les utilisateurs	Type de sécurité : VPA - Entreprise  Type de  chiffrement : AES	I
Me connecter au Me connecter à Me connecter m	utomatiquement lorsque ce réseau est à portée un réseau favori prioritaire si cela est possible ême si le réseau ne diffuse pas son nom (SSID)	Choisissez une méthode d'authentification réseau : Microsoft: PEAP (Protected EAP) ▼ Paramètres ✓ Mémoriser mes informations d'identification pour cette connexion à chaque fois que je suis connecté	
		Paramètres avancés	
	OK Annuler	OK. An	nuler

Erduan HOXHA 11 Dans l'onglet Sécurité de la fenêtre « Propriétés du réseau sans fil ... », vous devez vous rendre dans Paramètres (pour la méthode d'authentification réseau).

Une nouvelle fenêtre fait son apparition, vous devez alors décocher la case « Valider le certificat du serveur » (cocher par défaut) et sélectionner la méthode d'authentification : Mot de passe sécurisé (EAP-MSCHAP version 2) :

e de la connex	ion (			L.
	aon:			
Valider le ce	rtificat du serveu	r		
Connexion	à ces serveurs :			
Autorités de ce	ertification racine	de confiance :		
AddTrust	External CA Root			
Baltimore (	CyberTrust Root			
Class 3 Pu	blic Primary Certi	fication Authority		11
DigiCert A:	ssured ID Root C	A		
Equifax Se	cure Certificate	Authority		
GeoTrust (	Global CA			
📃 GlobalSign	Root CA			-
	11	1		•
Ne pas dem	ander à l'utilisate	eur d'autoriser de r	nouveaux	
Ne pas dem serveurs ou ectionner la m ot de passe sé Activer la reco	ander à l'utilisate a des autorités de éthode d'authent curisé (EAP-MSC ponnexion rapide	eur d'autoriser de r e certification appr ification : HAP version 2)	ouveaux ouvées.	nfigurer
Ne pas dem serveurs ou ectionner la m ot de passe sé Activer la reco Appliquer la p	ander à l'utilisate u des autorités de éthode d'authent curisé (EAP-MSC ponnexion rapide rotection d'accès	eur d'autoriser de r e certification appr ification : HAP version 2) réseau	ouveaux ouvées.	nfigurer
Ne pas dem serveurs ou ectionner la m ot de passe sé Activer la reco Appliquer la p Déconnect. si	ander à l'utilisate a des autorités de éthode d'authent curisé (EAP-MSC prinexion rapide rotection d'accès le serveur ne pri	eur d'autoriser de r e certification appr ification : HAP version 2) réseau ésente pas TLV de	iouveaux ouvées,	higurer.
Ne pas dem serveurs ou ectionner la m ot de passe sé Activer la reco Appliquer la p Déconnect. si Activer la pro la confidential	ander à l'utilisate des autorités de éthode d'authent curisé (EAP-MSC ponnexion rapide rotection d'accès le serveur ne pro tection de lité	eur d'autoriser de r e certification appr ification : HAP version 2) réseau ésente pas TLV de	iouveaux ouvées.	nfigurer. chiffr.

Ensuite cliquer sur Configurer et décocher la case « Utiliser automatiquement mon nom et mon mot de passe Windows ... » puis OK et enfin revenez sur la fenêtre « Propriétés du réseau sans fil ... » :



Rendez vous maintenant dans « Paramètres avancés », une nouvelle fenêtre s'ouvre, cocher « Spécifier le mode d'authentification » et choisissez « Authentification de l'utilisateur » :

Tvpe de sécurité :	WPA - Entreprise		Spécifier le mode d'authentificat	ion :		
Type de	[		Authentification de l'utilisateur	Enregistrer ident.		
chiffrement :	AES	•	U Supprimer les informations d'iden utilisateurs	tification pour tous les		
			Activer l'authentification unique	pour ce réseau		
Choisissez une méth	ode d'authentification ré	seau :	Immédiatement avant l'ouver	ture de session de l'utilisateur		
Microsoft: PEAP (Protected EAP)		Paramètres	Minimédiatement après l'ouvert	Immédiatement après l'ouverture de session de l'utilisateur		
Mémoriser mes in cette connexion	formations d'identificatio à chaque fois que je suis	on pour connecté	Délai maximal (secondes) ;	10		
			V Autoriser l'affichage de boîtes supplémentaires pendant l'aut	de dialogue thentification unique		
			Ce réseau utilise des réseaux l'authentification de l'ordinate	locaux virtuels distincts pour ur et de l'utilisateur		
Paramètres avanc	és					

Enfin Windows vous demande une authentification, c'est à ce moment qu'il faut entrer les données de l'utilisateur crée auparavant (l'utilisateur erduan dans notre cas) :

Authentifi	cation réseau	
Veuillez entre	r les informations d'identification util	isateur
	erduan	
1		Ξ.

Vous êtes désormais connecter à la borne wifi Erduan avec le protocole RADIUS :

Sélection	nner l'emplacement du réseau « Erduan »
Cet ordinat paramètres	teur est connecté à un réseau. Windows appliquera automatiquement les s réseau appropriés pour cet emplacement.
	Réseau domestique Si tous les ordinateurs de ce réseau sont à votre domicile et que vous les reconnaissez, il s'agit d'un réseau domestique approuvé. Ne choisissez pas cette option pour des endroits publics tels que des cybercafés ou des aéroports.
	Réseau de bureau Si tous les ordinateurs de ce réseau sont sur votre lieu de travail et que vous les reconnaissez, il s'agit d'un réseau de bureau approuvé. Ne choisissez pas cette option pour des endroits publics tels que des cybercafés ou des aéroports.
	Réseau public Si vous ne reconnaissez pas tous les ordinateurs du réseau (par exemple si vous êtes dans un cybercafé ou un aéroport, ou si vous disposez d'un haut débit mobile), il s'agit d'un réseau public et il n'est pas approuvé.
Traiter t	ous les réseaux auxquels je me connecterai à l'avenir comme des réseaux publics, et ne plus er la question.
Comment	choisir ?