# TP – WIFI RADIUS

# Exercice 1 - Configuration de la borne

- 1. Donner une adresse IP LAN et WAN à la borne ou routeur WIFI
- 2. Donner un nom au SSID
- 3. Tester la connexion entre la borne et le serveur RADIUS

### Paramétrage RADIUS de la borne

1. Choisir WPA2 entreprise, AES et le port 1812

# Exercice 2 - Paramétrage d'active directory et de Windows

- 1. Créer une OU RADIUS, dans laquelle on créé un groupe RADIUS, et un utilisateur Pierre (par exemple)
- 2. Dans les propriétés de l'utilisateur, activer l'option Contrôler l'accès via la Stratégie d'accès à distance
- 3. Dans le groupe RADIUS intégrer l'ordinateur portable, tablette, smartphone (sauf si smartphone autre que Windows) et l'utilisateur précédemment créé
- 4. Paramétrer le DNS en y ajoutant la borne
- 5. Installer IIS
- 6. Installer le service de certificats (voir TP IIS ou Tuto RADIUS) 7. Ajouter des rôles suivant au service de certificats
- Service Web Inscription de certificats
- Service Web Inscription de certificats
- Service Web Stratégie d'inscription de certificats

Vous sélectionnez la méthode d'accès « Authentification Intégrée Windows » au site web de certification

## Exercice 3 - Installation et gestion des certificats sur le serveur

#### Téléchargement du certificat de l'Autorité de certification

#### Adresse <a href="http://@ip">http://@ip</a> de mon serveur/certsrv

- 1. Choisir « télécharger un certificat d'autorité de certification ... »
- 2. Puis « télécharger un certificat d'autorité de certification »
- 3. Ouvrir et installer

### Demande de certificat pour le serveur RADIUS

Cette demande va être utile lors de l'échange entre le client WIFI la borne et le serveur RADIUS

- 1. Faire démarrer exécuter MMC
- 2. Ajouter composant logiciel enfichable Certificats
- 3. Choisir compte d'ordinateur (Ordinateur local)
- 4. Dans la console Certificat (Personnel), faire une demande de nouveau certificat
- 5. Choisir authentification contrôleur de domaine

# **Exercice 4 - Installation et gestion des certificats sur le serveur**

### Téléchargement du certificat de l'Autorité de certification

#### Adresse http://@ip de mon serveur/certsrv

- 1. Choisir « télécharger un certificat d'autorité de certification ... »
- 2. Puis « télécharger un certificat d'autorité de certification »
- 3. Ouvrir et installer

### Exercice 5 - Installation de NPS

Installation du service RADIUS

- 1. Installer le service de rôle Services de Stratégie et d'accès réseau
- 2. Dans les services cocher Serveur NPS

### Exercice 6 - Paramétrage de NPS

#### Choisir Serveur Radius pour les connexions sans fils 802.1X



# **Exercice 7 - Ajout d'un client RADIUS**

- 1. Donner un nom puis l'adresse IP de la borne et saisir le mot de passe préalablement saisi lors de la configuration de la borne
- 2. Choisir la méthode d'authentification Microsoft Carte à puce ou autre Certificat
- 3. Dans les propriétés choisir le certificat du serveur Radius

d'identité.	e certificat que vous voulez qu'il utilise comme pret
Certificat délivré à :	SVRADIUS.radius.local
Nom convigial :	
Émetteur :	radius-SVRADIUS-CA
Date d'expiration :	01/06/2013 13:47:44

- 4. Indiquer le groupe d'utilisateurs autorisé à faire une connexion WIFI
- 5. Inscrire le serveur dans AD

## Exercice 8 – RADIUS EAP/TLS

Mise en place de la configuration avec authentification par certificat client et certificat serveur

	Vue d'ensemble Conditions Contraintes Paramètres
	Configurez les contraintes de cette stratégie réseau.
	Contraintes :
	Contraintes
	A Méthodes d'authentification
	Délai d'inactivité Agne (Modern)
	Specific description de Sync (11 Line)
	ID de la station appelée
	Restrictions relatives aux     instructions during the second secon
	Type de port NAS Grade Ring
	Wireless - IEEE 802.11
	Dues     SSLCAP - Asymmetric DSL Camerless Amplitude Phase Modulation
	ADSL-DMT - Asymmetric DSL Discrete Multi-Tone
	Cable
1. Vér	ification des stratégies de connexion
	Stratégies de demande de connexion
	Les stratégies de demande de connexion vous permettent de spécifier si les demandes de
	connexion sont traitées localement ou si elles sont transférées vers des serveurs RADIUS distants. Pour les connexions NAP VPN ou 802.1X, vous devez configurer l'authentification PEAP dans la
	Nom de Catraite de demande de connexion Etat Ordre de traitement Source
	Connexions sans fil sécurisées 2 Activé 1 Unspecified     Unspecified     Unspecified
	Connexions sans fil sécurisées 2
	Conditions - Si les conditions suivantes sont réunies :
	Condition Valeur
	Type de port NAS Wireless - Other OU Wireless - IEEE 802.11
	Paramètres - Les paramètres suivants sont appliqués :
	Paramètres - Les paramètres suivants sont appliqués :
	Paramètres - Les paramètres suivants sont appliqués :         Paramètre       Valeur         Foumisseur d'authentification       Ordinateur local

#### 2. Vérification des stratégies réseau

p de la stratégie	État	Ordre de traitement	Type d'accès
Sinnexions sans fil sécurisées 2	Activé	1	Accorder l'ac
Connections to Microsoft Routing and Remote Access server	Activé	2	Refuser l'acc
Connections to other access servers	Activé	3	Refuser l'acc
		1	
Concernience some fill adouvindene 2			
Connexions sans in seconsees 2			
Conditions - Si les conditions suivantes sont réunies :			
Condition Valeur			
Type de port NAS Wireless - Other OU Wireless - IEEE 802 11			
Groupes Windows RADIUS\radius			
aramètres - Les paramètres suivants sont appliqués :			
Paramètres - Les paramètres suivants sont appliqués :	Vale	sur	
Paramètres - Les paramètres suivants sont appliqués : Paramètre Méthode d'authentification	Vale	sur iocole EAP OU MS-CH	1AP
Paramètres - Les paramètres suivants sont appliqués : Paramètre Méthode d'authentification Autorisation d'accès	Vale Prot Acc	sur locole EAP OU MS-CH order l'accès	1AP
aramètres - Les paramètres suivants sont appliqués : Paramètre Méthode d'authentification Autorisation d'accès Mettre à jour les clients non conformes	Vale Prot Acc Vrai	eur Pocole EAP OU MS-CH Porder l'accès	1AP
aramètres - Les paramètres suivants sont appliqués : Paramètre Méthode d'authentification Autorisation d'accès Mettre à jour les clients non conformes Contrainte de mise en conformité NAP	Vale Prot Acco Vrai Auto	sur locole EAP OU MS-CH order l'accès priser un accès réseau	HAP
aramètres - Les paramètres suivants sont appliqués : Paramètre Méthode d'authentification Autorisation d'accès Mettre à jour les clients non conformes Contrainte de mise en conformité NAP Framed-Protocol	Vale Prot Acc Vrait PPF	sur iocole EAP OU MS-CH iorder l'accès priser un accès réseau	HAP
aramètres - Les paramètres suivants sont appliqués : Paramètre Méthode d'authentification Autorisation d'accès Mettre à jour les clients non conformes Contrainte de mise en conformité NAP Framed-Protocol Service-Type	Vale Prot Acc Vrai Auto Fra	eur locole EAP OU MS-CH lorder l'accès priser un accès réseau ned	HAP
aramètres - Les paramètres suivants sont appliqués : Paramètre Méthode d'authentification Autorisation d'accès Mettre à jour les clients non conformes Contrainte de mise en conformité NAP Framed-Protocol Service-Type Ignorer les propriétés de numérotation des utilisateurs	Vale Prot Acc Vrai Auto PPF Fran Vrai	sur iocole EAP OU MS-CH iorder l'accès priser un accès réseau ned	1AP
Paramètres - Les paramètres suivants sont appliqués : Paramètre Méthode d'authentification Autorisation d'accès Mettre à jour les clients non conformes Contrainte de mise en conformité NAP Framed-Protocol Service-Type Ignorer les propriétés de numérotation des utilisateurs Méthode EAP (Extensible Authentication Protocol)	Vale Prot Vrai Auto PPF Fran Vrai Mici	eur cocole EAP OU MS-CH corder l'accès priser un accès réseau ned rosoft: Carte à puce ou	HAP
Paramètres - Les paramètres suivants sont appliqués : Paramètre Méthode d'authentification Autorisation d'accès Mettre à jour les clients non conformes Contrainte de mise en conformité NAP Framed-Protocol Service-Type Ignorer les propriétés de numérotation des utilisateurs Méthode EAP (Extensible Authentication Protocol) Configuration du profocole EAP (Extensible Authentication Protocol)	Vale Prot Acc Vrai Auto Fran Mici Di) Con	sur locole EAP OU MS-CH lorder l'accès priser un accès réseau ned rosoft: Carte à puce ou figuré	HAP

# **Exercice 9 - Configuration du client pout EAP/TLS**

#### Certificat de l'AC

- 1. Télécharger et installer le certificat de l'autorité de certification sur le portable
- 2. Lors de l'installation, prendre les options par défaut puis recommencer en installant manuellement le certificat dans le conteneur autorité de certification
- 3. Vérifier dans le navigateur qu'il est bien présent

#### **Certificat Utilisateur**

- 1. Demander un certificat utilisateur qui servira à l'authentification RADIUS
- 2. Vérifier dans le navigateur qu'il est bien présent

### Paramétrage de la connexion WIFI

Entrer les informat	ons relatives au réseau sans fil à ajouter	
Nom réseau :	radius	
Type de sécurité :	WPA2 - Entreprise	
Type de chiffrement :	AES	
Clé de sécurité :	Masquer les caractèr	es
🔽 Lancer automatiq	uement cette connexion	
🔲 Me connecter mê	me si le réseau ne diffuse pas son n <b>om</b>	
Attention : si vou risque.	sélectionnez cette option, la sécurité de votre ordinateur peut co	urir un

Connexion Sécurité		
Type de sécurité : Type de chiffrement :	WPA2 - Entreprise	• •
Choisissez une méthoo Microsoft: Carte à pu	de d'authentification rés ce ou autre certific 👻	seau : Paramètres
The first first first first first	stitle della dictertatica de	I DOGI
cette connexion à	chaque fois que je suis	connecté

- 1. Tester la connexion
- 2. Vérifier le fonctionnement

# Exercice 9 - RADIUS EAP/PEAP pour Smartphone

Configuration de la connexion WIFI avec mot de passe Client et certificat Serveur

## Sur le serveur

1. Créer une nouvelle stratégie réseau ou modifier l'ancienne

Image: Second	Configurez les contraintes de cette stratégie Si la demande de connexion ne répond pas ADIU Contraintes :	e réseau. s à toutes les contraintes, l'accès réseau est refusé.	Modifier les propriétés EAP Protégé	u  x
<ul> <li>Groupes de serve</li> <li>Stratégies</li> <li>Stratégies de de Stratégies de de Gestion d'accès ré Gestion d'accès ré</li> <li>Gestion des modèles</li> </ul>	urs f Contraintes Méthodes d'authentification ibrôle seau Délai d'inactivité Seau Délai d'expiration de session ID de la station appelée Pestrictons relatives aux jours et aux heures Type de port NAS	Autorisez l'accès uniquement aux clients qui s'auther spécifiées. Les types de protocoles EAP sort négociés entre les l'ordre dans lequel ils sort listés. Types de protocoles EAP : Microsoft: PEAP (Protected EAP) 4 Autorer Modifier Supprimer Méthodes d'authentification chiffrée Morsoft version 2 (MS- V L'utilisateur peut modifier le mot de passe apré Authentification chiffrée (CHAP) L'utilisateur peut modifier le mot de passe apré Authentification chiffrée (CHAP) Authentification chiffrée (CHAP) Authentification chiffrée (CHAP) Authentification non chiffrée (PAP, SPAP) Authentification non chiffrée (PAP, SPAP) Authentification non trisfrée de l'ordinateur	Sélectionnez le certificat que le serveur doit utiliser comme p         identité auprès du client. Un certificat configure pour BAP en         stratégie de demande de connexion remplacera ce certificat         Certificat délivré à :       SVRADIUS radius local         Nom convivial :         Émetteur :       radius-SVRADIUS-CA         Date d'expiration :       01/06/2013 13:47:44         IV Activer la reconnexion rapide         Déconnecter les clients sans chiffrement forcé         Types EAP         Mot de passe sécurisé (EAP-MSCHAP version 2)         Ajouter       Modifier	reuve de son obégé dans la Morter Dessendre Annoler
R	0		OK Annuler Appliquer	

### Sur le client

