Utilisation PEAP MS-CHAPV2

Pourquoi :

Pour avoir l'authentification machine et utilisateur Utilisateur authentifié par son mot de passe / login AD Pas de clé à installer sur les postes

Mise en oeuvre :

Le point d'accès est un WRT54GS V4 avec firmware dd-wrt 0,23

Coté serveur :

Sur un contrôleur de domaine, installer :

- IIS

- Service d'authentification internet
- Certificat
- Configurer le routage et accès distant (pour utiliser DHCP sur les postes en wifi)

<u>Résultat :</u>

L'authentification par couple login mot de passe fonctionne, il y a descente des profils et exécution des scripts de connexion.

Les GPO machines et utilisateurs sont prises en compte à condition d'ajouter la clé suivante dans la base de registre :

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters

Clé de type REG_DWORD : DisableDHCPMediaSense Mettre la valeur 1

Le processus de BOOT est alors beaucoup plus long, mais tous les paramètres machine sont correctement installés.

Ce mode de connexion wifi est vulnérable aux attaques avec des couples mot de passe / login donc dans les paramètres de sécurité, désactiver les comptes après 5 tentatives infructueuses d'ouverture de session pendant 5 min par exemple. De plus refuser le wifi aux utilisateurs ayant des privilèges administrateur sur le domaine.

Important : toutes les affirmations de ce document doivent être complétées par : "pour autant que je sache"

PEAP MS CHPA-V2

Ici, le client s'assure de l'identité du serveur radius par un certificat sur celui-ci.

Par contre, tout utilisateur capable de fournir un couple login / mot de passe, validé par radius, sera accepté sur le réseau.

Cela implique, qu'il est prudent de limiter les comptes acceptés par radius, en particulier, les administrateurs du domaine ne devraient pas utiliser une station en wifi pour administrer le réseau.

Le serveur radius communique avec le point d'accès grâce à l'adresse IP de celui et une clé partagée qui doit être robuste.

Il est important de configurer les clients afin qu'ils refusent la connexion à un serveur radius qui n'a pas de certificat, ceci afin d'éviter qu'un pirate tente de se faire passer pour un point d'accès et intercepte toutes les communications du client.

Le mécanisme d'ouverture de session est sûr, les échanges sont cryptés et ne sont pas analysables (19/12/2006) ensuite, la session est cryptée en WPA-AES ou bien WPA-TKIP qui est un peu moins robuste mais toujours considéré comme non cassable. On peut mixer les deux (TKIP+AES)

Pour améliorer la sécruité de l'ensemble, j'ai imposé la signature SMB sur les clients wifi. (je ne suis pas certain du grand interet de la chose...)

EAP-TLS

L'EAP-TLS demande l'installation de certificats sur la machine, pour identifier la machine et pour l'utilisateur. C'est un peu lourd à gérer par contre, c'est très sûr.

WPA – PSK

Demande l'installation de clés partagées entre le point d'accès et les stations, si la clé du point d'accès est compromise, il faut repasser sur toutes les stations. On ne peut pas filtrer les utilisateurs qui se connectent en wifi.

Deux cryptages sont proposés :

TKIP, compatible avec le matériel utilisant le cryptage WEP AES plus performant

Parfois on a l'option TKIP+AES sur le point d'accès ce qui donne la possibilité d'utiliser des clients avec les deux types de cryptage

Installation de l'autorité racine

Pour initier une ouverture de compte , il faut une communication sécurisée, un tunnel crypté. Pour cela le protocole PEAP – MS CHAP V2 demande un certificat serveur qui sera validé au niveau du client (on valide l'autorité de certification).

L'installation de l'autorité racine est parfaitement détaillée sur ce lien : <u>http://www.laboratoire-microsoft.org/articles/network/wpa/3/</u>

Installation d'IAS

Le serveur radius, est un des services proposé par IAS, il faut donc installer ce service. L'installation se fait par : ajout / suppression de programmes => Ajouter supprimer des composants Windows => Services de mise en réseau => Service d'authentification Internet.

Lancer la console services et authentification internet

Ajout du client

Il y a autant de clients que de points d'accès, y penser lorsque l'on nomme son client.



Adresse IP du point d'accès ou son nom, s'il est enregistré dans DNS, le bouton « vérifier » permet de faire une résolution DNS.

Nom convivial : Nom qui apparaîtra dans la console IAS

Entrez un nom convivial et soi	it une adresse IP, soit un nom	DNS pour le client.
<u>N</u> om convivial :	wifi wrt54g	
Adresse du client (IP ou DNS)	l:	
192.168.1.1		Vérifier

Le secret est partagé entre le point d'accès et le serveur Radius, il doit être robuste.

nformations supplémentaires	
Si vous utilisez des stratégies d'acc spécifiez le fournisseur du client R/ Olient-Fournisseur :	cès à distance basées sur l'attribut client-fournisseur, ADIUS.
RADIUS Standard	•
S <u>e</u> cret partagé :	*****
Confirmer le secret partagé :	***************************************
Les requêtes doivent <u>c</u> onten	ir l'attribut de l'authentificateur de message

Que dire de la case à cocher ?

Méthode de c	onfiguration de stratégie
L'Assistant j	peut créer une stratégie typique ou vous pouvez créer une stratégie
personnalis	ée.
Comment vo	ulez-vous paramétrer cette stratégie ?
Utiliser	cet Assistant pour paramétrer une stratégie par défaut pour un scénario commun
C <u>I</u> nstalle	r une stratégie personnalisée
Entrez un nor	a qui décrit cette stratégie
Entrez un nor	n qui décrit cette stratégie.
<u>N</u> om de la	accès wifi voillaume
Entrez un nor	n qui décrit cette stratégie.
<u>N</u> om de la	accès wifi voillaume
stratégie :	Exemple : authentifie toutes les connexions VPN.
Entrez un nor	n qui décrit cette stratégie.
<u>N</u> om de la	accès wifi voillaume
stratégie :	Exemple : authentifie toutes les connexions VPN.

On utilise l'assistant et on donne un nom à cette stratégie, c'est le nom qui apparaîtra dans la console IAS.

istant 9	Stratégie de nouvel accès à distance
Métho Les rése	de Access : conditions de la stratégie sont basées sur la méthode utilisée pour accéder au eau.
Sélec	tionnez la méthode d'accès pour laquelle vous voulez créer une stratégie.
C	<u>⊻</u> PN
	Utiliser pour toutes les connexions VPN. Pour créer une stratégie pour un type de VP spécifique, retourner à la page précédente et sélectionner Installer une stratégie personnalisée.
С	A <u>c</u> cès à distance
	Utiliser pour les connexions d'accès à distance qui utilisent des lignes téléphoniques traditionnelles ou une ligne RNIS.
œ	Sanshi
	Utiliser pour des connexions réseau sans fil uniquement.
С	<u>E</u> thernet
	Utiliser pour des connexions Ethernet, telles que des connexions utilisant un commutateur.
	< <u>P</u> récédent <u>S</u> uivant > Annule

C'est une stratégie pour du sans-fil

ssistant Stratégie de nouvel accès à distance	X
Accès utilisateur ou de groupe Vous pouvez accorder l'accès à des utilisateurs indivi accorder l'accès à des groupes sélectionnés.	iduels ou vous pouvez
Accorde l'accès selon le choix suivant : Utilisateur Les autorisations d'accès utilisateurs sont spécifiées Groupe Les autorisations d'un utilisateur individuel l'emporte : <u>N</u> om du groupe :	dans le compte d'utilisateur. sur les autorisations d'un groupe.
VOILLAUME\Ordinateurs du domaine VOILLAUME\Utilisa. du domaine	Ajouter Supprimer
< <u>P</u> récé	édent <u>Suivant ></u> Annuler

Je pense qu'il faut mettre les ordinateurs du domaine afin que le réseau soit monté avant l'ouverture de session. L'ordinateur s'authentifie à radius et peut donc exécuter la partie machine des gpo (scripts, sécurité, etc.) j'y reviendrai.

Attention, le protocole est vulnérable à une attaque sur dictionnaire de mot de passe ou une attaque en brute. Le réseau étant accessible d'un point extérieur, on peut essayer de se connecter avec des couples login / mot de passe.

Je pense qu'il est préférable de ne laisser l'accès qu'aux profs et élèves voir restreindre en fonction des classes.

Les administrateurs du domaine, ne devraient pas pouvoir accéder au réseau via le wifi

Il est également possible de créer un groupe Wifi, dans lequel on mettra les ordinateurs et les utilisateurs autorisés à utiliser le wifi.

Assistant Stratégie de nouvel accès à d	listance	×
Méthodes d'authentification EAP utilise différents types de périphér utilisateurs.	riques de sécurité pour authentifier des	ŷ
Séle <u>c</u> tionnez le type d'EAP pour cette s <u>T</u> ype : PEAP (Protected EAP)	stratégie.	rer
	< <u>P</u> récédent <u>S</u> uivant >	Annuler

Ici on choisi PEAP et on configure

Propriétés EAP protége	ées	? ×
Ce serveur s'identifie au réalisée. Sélectionnez le d'identité.	orès des appelants avant que la connexion ne soit certificat que vous voulez qu'il utilise comme preuv	e
⊆ertificat délivré à :	srv-etk-2003.voillaume.local	•
Nom convivial :		
Émetteur :	root voillaume	
Date d'expiration :	04/12/2007 21:56:21	
Activer la reconnexio	n rapide	
Types EA <u>P</u>		25
Mot de passe sécurité (l	EAP-MSCHAP version 2)	onter
	Des	cendre
Ajouter Moo	ifjer <u>S</u> upprimer OK Ar	nuler

Il faut indiquer ici qui est l'autorité qui détient le certificat

On clique sur OK.

🎾 Service d'authentification Internet		
Eichier Action Affichage ? ← → € 🖬 🗙 🕾 🗟 😵 + +		
Service authentification Internet (local)	Nom	0 A
Connexion par accès distant	S Connexions au serveur d'accès à distance et d	2
 Brategies d'acces distant 	S Connexions à d'autres serveurs d'accès	3

Les stratégies sont examinées les unes après les autres, dès qu'un accès est autorisé, on arrête. Sinon, on examine la stratégie suivante. Il faut donc laisser ces deux stratégies qui in fine bloquent l'accès au réseau sans fil.

On va ensuite dans propriétés de la stratégie, pour configurer deux ou trois petites choses :

Spécifiez les co	nditions que les de	mandes de connexion	doivent remplir.
<u>C</u> onditions de la	stratégie :		
NAS-Port-Type	égale "Sans fil - A	utre OR Sans fil - IEEE	802.11" AND
Windows-Group	ps égale "VOILLAI	JME\Ordinateurs du do	omaine;VOILLAUN
•			•
Aioutor	Medifier	Supprimer	
Alguter			
Si les demandes	de connexion cor	respondent aux conditi	ons spécifiées
dans cette strate	egie, le profil assoc	xe sera applique a cetti	e connexion.
Medifier le prot	äl		
Mouner le proi			
À moins que des stratégie contrôl	s autorisations d'ac ent l'accès au rése	ces individuelles solen au	t specifiees, cette
À moins que des stratégie contrôl	s autorisations d'ac ent l'accès au rése	ces individuelles solen 3au.	t specifiees, cette
À moins que des stratégie contrôl Si une demande	s autorisations d'ac ent l'accès au rése de connexion est	conforme aux conditio	r specifiées : ns spécifiées :
À moins que des stratégie contrôl Si une demande C <u>B</u> efuser l'au	s autorisations d'ac ent l'accès au rése : de connexion est :orisation d'accès (conforme aux conditio distant	t specifiées, cette ns spécifiées :

et l'on clique sur modifier le profil

Contraintes pour les appels e	entrants	IP	Liaisons multiples
Authentification	Cryptage	1	Paramètres avancés
ectionnez les méthodes d'auti	hentification que	vous voulez a	autoriser pour cette connexio
Méthodes <u>E</u> AP			
Authentification cryptée Mi	icrosoft version <u>2</u>	(MS-CHAP v.	2)
🔲 L'utilisateur peut mo	difier le mot de pa	isse après sor	n expiration
Authentification cryptée Mi	icrosoft (MS-CHA	P)	
📕 L'utilisateur peut mo	difier le mot de pa	isse après sor	n expiration
Authentification cryptée (C	HAP)		
Authentification non crypté	ée (PAP, SPAP)		
Accès non authentifié			
Autoriser les clients à se cr	onnecter sans né	aocier une m	éthode d'authentification
		goolor and m	

Que dire de : "l'utilisateur peut modifier le mot de passe après expiration" ?

Modifier un profil d'appel entrant	? ×
Contraintes pour les appels entrants IP Authentification Cryptage	Liaisons multiples Paramètres avancés
Les niveaux de cryptage suivants sont pris en charge par des serv routage et d'accès distant Microsoft. Si vous utilisez un autre serve que les niveaux de cryptage sélectionnés sont pris en charge par o Si Aucun cryptage est la seule option sélectionnée, les utilisateurs connecter en utilisant le cryptage de données	eurs exécutant le service de eur d'accès réseau, vérifiez ce serveur. ne peuvent pas se
Aucun cryptage	
🔲 Cryptage de <u>b</u> ase (MPPE 40 bits)	
Cryptage renforcé (MPPE 56 bits)	
Cryptage maximal (MPPE 128 bits)	
ОК	Annuler <u>A</u> ppliquer

Dans l'onglet cryptage, je n'ai laissé que 128 bits, ce qui doit imposer une version de IE avec le cryptage 128 bits.

Dans un premier temps, j'avais tout laissé afin de ne pas avoir une source de blocage ici.

Enfin, ne pas oublier les logs (sinon Fabrice va me tuer !)



opriétés de Fichier loc	al	?
Paramètres Fichier journ	al]	
Enregistrer les informatio	ns suivantes :	
Requêtes de gestion de compte)	n de compte (par exemple : c	ouverture ou fermeture
🔽 <u>R</u> equêtes d'authenti	fication (par exemple : accè:	s accepté ou refusé)
Statut <u>p</u> ériodique (pa intérim)	ar exemple, les requêtes de <u>c</u>	gestion de compte par
		1
	OK Ar	nnuler <u>A</u> ppliquer

Propriétés de Fichier local	? ×
Paramètres Fichier journal	
Nom : Taslog.log <u>R</u> épertoire :	
C:\WINDOWS\system32\LogFiles	Parcourir
<u>F</u> ormat :	
o jas	
Compatible avec les bases de données	
Créer un nouveau fichier journal :	
C Tous les jours	
C Toutes les <u>s</u> emaines	
C Tous les <u>m</u> ois	
O Jamais (taille de fichier <u>n</u> on limitée)	
Lorsque le fichier journal atteint cette <u>t</u> aille : 10	Mo
Lorsque le disque est plein, supprimer les anciens fichie	rs journaux
OK Annuler	Appliquer

Si l'on veut utiliser DHCP pour ses clients sans fil, il faudra configurer le routage et accès distant.

Lancer routage et accès distant dans outils d'administration.

🚊 Routage et accès distant	SRV-ETK-2003 (local)
État du serveur SRV-ETK-2003 (local) <u>Configurer e</u> <u>Désactiver l</u> <u>T</u> outes les t Affic <u>h</u> age <u>S</u> upprimer Act <u>u</u> aliser	Configurer le serveur de Routage et d'accès distant t activer le routage et l'accès distant l'accès distant, cliquez Configurer et Activer aches •
Assistant Installation Configuration Vous pouvez ac personnaliser ce	du serveur de routage et d'accès distant tiver l'une des combinaisons de services suivantes ou vous pouvez serveur.
 Accès à dist Autoriser les distance, une NAT (Netwo Autoriser les Accès VPN Autoriser les locaux à se d Connexion s Connecter ce Configuration Sélectionner distant. 	ance (connexion à distance ou VPN) clients distants à se connecter à ce serveur via une connexion d'accès à e connexion Internet sécurisée ou une connexion réseau privé virtuel (VPN). rk address translation) clients internes à se connecter à Internet en utilisant une adresse IP publique. <u>Wirtual Private Network) et NAT</u> clients distants à se connecter à ce serveur par Internet et les clients connecter à Internet en utilisant une seule adresse IP publique. écurisée entre <u>d</u> eux réseaux privés e réseau à un réseau distant tel que la succursale d'un bureau. In personnalisée une combinaison de fonctionnalités disponibles dans Routage et accès rmations, consultez l' <u>Aide du Routage et de l'accès distant</u> .
	< <u>P</u> récédent <u>S</u> uivant > Annuler

ssistant Installation du serveur de routage et d	'accès distant
Accès distant Vous pouvez configurer ce serveur pour recevoir connexions d'accès à distance.	des connexions VPN et des
☑ VPN Un serveur VPN (aussi appelé passerelle VPI connexions à partir de clients distants via Inter	N) peut recevoir des ernet.
Accès à distance Un serveur d'accès à distance peut recevoir clients à distance via un média d'accès à dis	r des connexions à partir de stance tel qu'un modem.
	< <u>P</u> récédent <u>S</u> uivant > Annuler

Assistant Installation du serveur de routage et d'accès distant	
Attribution d'adresses IP Vous pouvez sélectionner la méthode d'assignation des adresses IP aux clients.	
Comment voulez-vous que les adresses IP soient attribuées aux clients distants ?	
Si vous utilisez un serveur DHCP pour attribuer des adresses, confirmez qu'il est configuré correctement. Si vous n'utilisez pas de serveur DHCP, ce serveur générera les adresses.	
A partir d'une plage d'adresses spécifiée	
< <u>Précédent</u> <u>Suivant</u> >	Annuler

tien que le Routage et l'accès à distance permettent l'authentification de requêtes de connexion, des réseaux importants incluant plusieurs serveurs d'accès à distance utilisent ouvent un serveur RADIUS pour centraliser l'authentification. ii vous utilisez un serveur RADIUS sur votre réseau, vous pouvez paramétrer ce erveur pour transférer les requêtes d'authentification au serveur RADIUS. 'oulez-vous configurer ce serveur pour travailler avec un serveur RADIUS ?	Des requêtes de connexion peuvent être a serveur RADIUS (Remote Authentication D	uthentifiées localement ou transférées à un ial-In User Service) pour être authentifiées.
ii vous utilisez un serveur RADIUS sur votre réseau, vous pouvez paramétrer ce erveur pour transférer les requêtes d'authentification au serveur RADIUS. 'oulez-vous configurer ce serveur pour travailler avec un serveur RADIUS ?	Bien que le Routage et l'accès à distance p connexion, des réseaux importants incluant souvent un serveur RADIUS pour centralise	ermettent l'authentification de requêtes de plusieurs serveurs d'accès à distance utilisent r l'authentification.
oulez-vous configurer ce serveur pour travailler avec un serveur RADIUS ?	Si vous utilisez un serveur RADIUS sur votr serveur pour transférer les requêtes d'authe	e réseau, vous pouvez paramétrer ce ntification au serveur RADIUS.
	Voulez-vous configurer ce serveur pour trav	ailler avec un serveur RADIUS ?
Non, utiliser Routage et accès à distance pour authentifier les requêtes de connexion	O <u>N</u> on, utiliser Routage et accès à distanc	e pour authentifier les requêtes de connexion
Qui, configurer ce serveur pour travailler avec un serveur RADIUS	💿 Qui, configurer ce serveur pour travailler	avec un serveur RADIUS

Assistant Installation du serveu	r de routage et d'accès distant	
Sélection du serveur RADIU Vous pouvez spécifier les ser l'authentification et la gestion	I S veurs RADIUS que vous voulez utiliser pour des comptes.	P
Entrez les serveurs RADIUS gestion des comptes et l'auth Serveur <u>R</u> ADIUS principal : Serveur radius s <u>e</u> condaire : Entrez le mot de passe qui es Se <u>c</u> ret partagé :	principal et secondaire que ce serveur utilisera pour la entification à distance. srv-etk-2003 t utilisé pour contacter ces serveurs RADIUS.	
		Annulei

On peut installer un serveur radius secondaire, mais je ne sais pas comment indiquer à mon point d'accès un deuxième radius...

	Fin de l'Assistant Installation du serveur du routage et d'accès distant	
	Vous avez configuré ce serveur en tant que serveur d'accès distant.	
	Résumé :	
outage et accès distant		×
	OK Aide	
	Pour fermer cet Assistant, cliquez sur Terminer.	

Le service prend en charge, le relais DHCP.

Je vais ensuite dans propriétés

Eichier Action Afficha	oe 2 ≌ ͡͡͡͡][[
Routage et accès dista	nt	SRV-ETK-2003 (local)	
Brv-ETK-2003 (lo	<u>C</u> onfigure <u>D</u> ésactive	r et activer le routage et l'accès distant r le routage et l'accès distant	ta n
Routage IP Général Général	Toutes les tâches		► Z
	Affichage		•
Agent de	<u>S</u> upprimer Act <u>u</u> aliser		
	P <u>r</u> opriété:	5	
	Aide		

Pour configurer la sécurité :

ropriétés de SRV-ETK-2003 (local)	? ×			
Général Sécurité IP PPP Enregistrement				
Le fournisseur d'authentifications valide les informations (les clients d'accès distant et les routeurs de connexion à	d'identification pour la demande.			
Eournisseur d'authentifications :				
Authentification RADIUS	Configurer			
<u>M</u> éthodes d'authentification Le fournisseur de comptes conserve un journal des demandes de connexions et des sessions.				
Fournisseur de comptes :	Canfigurar			
Gestion de comptes RADIUS				
La stratégie IPSec personnalisée spécifie une clé pré-pa connexions L2TP. Le service de routage et d'accès dista démarré pour définir cette option. Autoriser la stratégie IPSEC personnalisée pour les c Clé pré-partagée :	rtagée pour les ant doit être onnexions <u>L</u> 2TP			
Annue				

ropriété	≦s de SR¥-ETK	-2003 (loc	al)		?>
Général	Sécurité IP	PPP	Enreg	istrement	
Méthoo	les d'authenti	fication			? ×
Le ser sélecti	veur authentifie l ionnées dans l'or	es système: dre qui app	s distants araît ci-de	en utilisant les essous.	méthodes
I▼ <u>P</u> re	otocole EAP (Ex	tensible Aut	henticatio	n Protocol)	
	Méthodes <u>E</u> AP				
🔽 Au	thentification cry	ptée Micro:	soft <u>v</u> ersio	n 2 (MS-CHAP	9 v.2)
🗖 Au	thentification cry	ptée Micros	soft (MS-C	(HAP)	
E Au	Ithentification cry	ptée (CHAP	P)		
	otocole SPAP (S	hiva Passw	ord Authe	entication Proto	icol)
<u>M</u>	ot de passe non	crypté (PAF	9		
Acce	ès non authentifi	é			
Г.	Autoriser les sys	tèmes distar	ntsàse c	onnecter sans	authentification
					12
				UK	Annuler
2					
2			ок	Annuler	

Finalement, pour le débogage. Noter que le suivi se trouve dans %WINDIR%\TRACING

Propriétés de SRV-ETK-2003 (local)	<u>?</u> ×
Général Sécurité IP PPP Enregistrement Sélectionnez les types d'événements que vous voulez enregistrer : Enregistrer uniquement les erreurs dans le journal Enregistrer les erreurs et les avertissements Enregistrer tous les événements Ne pas rentrer g'événements Enregistrer les informations d'Accès à distance et routage supplémentaires (utilisées pour le débogage) Pour afficher les informations contenues dans ces fichiers journaux, ouvrez le répertoire de suivi %windir%\tracing.	
OK Annuler App	oliquer

Configuration des clients (portables par exemple)

La configuration peut se faire au niveau des stratégies, ou directement sur chacun des portables. Si l'on configure au niveau des stratégies avec une OU qui contient les portables par exemple il y aura juste à brancher une fois le portable sur le réseau avec un cordon réseau, pour qu'il prenne sa stratégie et c'est tout !

Configuration au niveau stratégies

⊞ · · · · · · · · · · · · · · · · · · ·			
Etratégies de clé publique	⊆réer une stratégie de réseau sans fil…		
 Stratégies de restriction logicielle Stratégies de sécurité IP sur Active Director - 	Toutes les tâches		
Modèles d'administration	Act <u>u</u> aliser		
Configuration utilisateur Paramètres du logiciel	Aide		
Assistant Stratégie de réseau sans fil Nom de stratégie de réseau sans fil Entrez un nom et une brève description pour cette s	stratégie de réseau sans fil.		
wifi portable			
Description :			
configurations des clients wifi			
< <u>P</u> rév	cédent <u>S</u> uivant > Annuler		

On donne ici le nom de la stratégie.



À la fin de la création de la stratégie, on nous propose de la configurer.

opriétés de wifi po	rtable	? ×
Général Réseaux fa	avoris	
<u>N</u> om :		
wifi portable		
Description :		
configurations des	clients wifi	4
⊻érifier les modificat 180 min	ions de stratégies toutes les : utes	
<u>A</u> ccès réseau :	Réseaux avec point d'accès u	iniquement (infrastruc 💌
☑ <u>U</u> tiliser Window: □ Se connecter a	s pour configurer les paramètres ré: utomatique <u>m</u> ent aux réseaux non f	seau sans fil pour les clients avoris
		OK Annuler

On ajoute un réseau wifi

Propriétés de wifi portable	Propriétés de Nouveau paramètre de préférence
Général Réseaux favoris	Propriétés du réseau IEEE 802.1x
	Nom réseau (SS <u>I</u> D) :
Connexion automatique aux réseaux disponibles dans l'ordre indiqué ci-dessous.	reseauvoillaume@free.fr
	Description :
Réseaux :	wifi voillaume
Nom réseau (SSID) IEEE 802.1x Cryptage Monter Descendre Descendre	Clé de réseau sans fil Authentification réseau : WPA Cryptage des données : AES La clé est fournie automatiquement Ceci est un réseau d'égal à égal (ad hoc) ; les points d'accès sans fil ne sont pas utilisés
OK Ann	uler OK Annuler

Et on configure le 802.1x

opriètes du re	éseau IEE	E 802.1x		
Z Contrôle d	'accès rése	au utilisant IEEE 802.1X		
<u>M</u> essage EAF	POL-Start :	Transmission	•	
Paramètres	secondes)-	- 577		
Ма <u>х</u> .:	3	Péri <u>o</u> de de	60	
	100	démarrage :		
Période de maintien :	160	Période d'authentification :	30	
	S.			
			Paramètres.	••
Authentifi	er en tant di	l'invité lorsque les informatio	ns concernant	
	ur ou l'utilisal	teur ne sont pas disponibles	ns concernant	
l'ordinateu		u'ordinateur lorsque les inforr	mations de	
l'ordinate	er en tant qu			
l'ordinateu Authentifi l'ordinateu	er en tant qu ur sont dispo	oni <u>b</u> les		
l'ordinateu Authentifi l'ordinateu Aut <u>h</u> entificati ordinateur :	er en tant qu ur sont dispo on de	oni <u>b</u> les Ordinateur uniquement		

Ici je suis un peu paumé je me contente de choisir type PEAP et d'aller dans paramètres

Que dire du message EAPOL-START ?

Que dire des trois options pour l'authentification de l'ordinateur ?

Ici, on valide l'autorité de certification :

Propriétés EAP protégées	? ×
Lors de la connexion :	
_ 🔽 Valider le certificat du serveur	
Conne <u>x</u> ion à ces serveurs :	_
Autorités de certification racines de confiance :	12
 NetLock Expressz (Class C) Tanusitvanykiado NetLock Kozjegyzoi (Class A) Tanusitvanykiado NetLock Uzleti (Class B) Tanusitvanykiado PTT Post Root CA root voillaume root voillaume 	
Saunalahden Serveri CA	<u>ا</u> لا
Ne pas demander à l'utilisateur d'autoriser de nouveaux serveurs ou des autorités de certification approuvées. Sélectionner la méthode d'authentification :	
Mot de passe sécurité (EAP-MSCHAP version 2)	urer
Activer la reconnexion rapide	
OK An	nuler

Pourquoi deux certificats / serveurs ici ?

On active la reconnexion rapide (pour un changement de point d'accès, je crois).

On vérifie que dans configurer, la case est bien cochée

Propri	étés EAP MSCHAPy	2	×
Lors	de la connexion :		
4	Utiliser automatiquem passe <u>W</u> indows d'ou éventuellement le do	ent mon nom et mo verture de session (maine)	n mot de jet
	[OK]	Annuler	

seaux :			
om réseau (SSID) reseauvoillaume@	IEEE 802.1x Activé	Cryptage AES	Mo <u>p</u> ter Descendre

Toutes les options présentes ici ne se retrouvent pas dans la configuration réseau de l'ordinateur ?



Cette partie n'est pas nécessaire dans le cadre d'une authentification MS-CHAP V2

Par contre, elle peut être utilisée en EAP TLS que je n'ai pas testé

Configuration de l'inscription automatique des certificats ordinateurs

Elle permet d'installer un certificat machine automatiquement.



La prochaine fois qu'un ordinateur ouv modèle que vous aurez sélectionné se	vrira une session, un certificat base sur le era fourni.
Un modèle de certificat est un ensemb délivrés aux ordinateurs. Choisissez ur Modèles de certificats :	ele de propriétés prédéfinies pour des certificats n modèle dans la liste suivante.
Nom	Rôles prévus
Agent d'inscription (ordinateur) Contrôleur de domaine IPSEC Ordinateur	Agent de demande de certificat Authentification du client, Authentification d Sécurité IP IKE intermédiaire Authentification du client, Authentification d
•	<u> </u>

Fin de l'Ass demandes certificats	de certificats sistant Création de automatiques de	2
Vous avez correcte demandes automati Le modèle de certifi	ment terminé l'Assistant Création iques de certificats. cat que vous avez sélectionné e	de st
affiché ci-dessous : Nom	Ordinateur	



Configuration du point d'accès :

Pas grand chose à mettre sur le point d'accès, la clé partagée avec le serveur radius. L'adresse IP du serveur radius (le serveur avec IAS IIS, etc.) Le port donné ici est celui par défaut de Windows 2003

Sécurité Sans Fil		
Cryptage Sans Fil		
Mode de Sécurité	WPA RADIUS	•
Cryptage WPA	AES 💽	
IP du serveur RADIUS	192, 168, 1,	100
Port du serveur RADIUS	1812	(Défaut: 1812)
Clé WPA partagée	•••••	Afficher
Délai de renouvellement des clés (en	3600	
seconds)		

192,168,1,10 = IP serveur ETK hébergeant IAS, certificats, AD

Configuration du client à la main (sans passer par les GPO)

Pour vérifier que ç marche pour le premier portable.

🚣 Propriétés de Connexion au réseau local	<u>?</u> ×
Général Authentification Avancé	
Sélectionnez cette option pour fournir l'accès réseau authentifié à des réseaux Ethernet.	
Activer l'authentification IEEE 802.1X pour ce réseau	
Type EAP : PEAP (Protected EAP)	
<u>P</u> ropriétés	
Authentifier en tant qu'ordinateur lorsque les informations de l'ordinateur sont disponibles	
Authentifier en tant qu'invité lorsque les informations concernant l'ordinateur ou l'utilisateur ne sont pas disponibles	
OK A	nnuler

Propriétés EAP protégées	? ×
Lors de la connexion :	
Connexion à ces serveurs :	 _
Autorités de certification racines de confiance :	
 Microsoft Root Certificate Authority NetLock Expressz (Class C) Tanusitvanykiado NetLock Kozjegyzoi (Class A) Tanusitvanykiado NetLock Uzleti (Class B) Tanusitvanykiado PTT Post Root CA root voillaume root voillaume 	 ▲ Propriétés EAP MSCHAPv2 ▲ Lors de la connexion : ■ Utiliser automatiquement mon nom et mon mot de passe Windows d'ouverture de session (et éventuellement le domaine)
serveurs ou des autorités de certification approuvées.	UK Annuler
Sélectionner la méthode d'authentification : Mot de passe sécurité (EAP-MSCHAP version 2)	Jrer
Activer la reconnexion rapide	short short
OK Ann	

÷.

Gestion du sans-fil par stratégies de groupe :



On a ici plusieurs options pour traiter les stratégies :

La détection d'une liaison lente de stratégie de groupe annule une partie des éléments des stratégies

Le seuil est à 500 Kbps soit 0,5 Mbps ce qui sur un point d'accès 54 Mbps ne devrait pas poser de problème.

On peut agir de deux façons pour modifier cela

- le seuil de détection de liaison (ou tout simplement désactiver la détection de liaison lente
- la prise en compte ou non des parties de stratégie en cas de liaison lente

Les paramètres de sécurité ne peuvent pas être désactivés

Ce tableau indique si la partie de stratégie est prise en compte en :

Liaison lente : si la liaison lente était détectée

peut être forcé : on peut les GPO, forcer l'application de ces parties de GPO même si une liaison lente est détectée

Arrière-plan : partie des GPO régulièrement mises à jour (via GPO) : contrôlable via GPO

Paramètre	(liaison lente) (peut être forcé)	Arrière-plan par défaut (via GPO)
Maintenance d'IE	(Non) (Oui)	OUI
Installation logicielle	(NON) (NON)	Non (NON)
redirection de dossier	(NON) (NON)	Non (NON)
scripts	(NON) (OUI)	Oui
sécurité IP	Non (OUI)	
stratégie sans fil	Non (OUI)	OUI
Récupération EFS		
Quotas de disque		OUI
Paramètre machine	Non (OUI)	OUI

Quelques liens :

 $\underline{http://www.microsoft.com/windows2000/fr/server/help/default.asp?url=/windows2000/fr/server/help/sag_RASS_MSCHAPv2.htm}{}$

http://www.schneier.com/paper-pptpv2-fr.html

http://www.informit.com/guides/content.asp?g=security&seqNum=72&rl=1

http://phares.ac-rennes.fr/_fichiers_/seriaE/admin/Telech/WiFi_PresentationDAIP.pdf