

Table des matières

CHAPITRE 1

Pourquoi une authentification sur réseau local ?	1
L'évolution des architectures de réseau	1
Nouveau paramètre pour la sécurité des réseaux sans fil	2
Les nouvelles solutions de sécurité	3
Radius, le chef d'orchestre	3
L'unification des méthodes d'authentification	4
Les protocoles étudiés dans cet ouvrage	4
En résumé... ..	5

CHAPITRE 2

Matériel nécessaire	7
Les équipements réseau	7
Rappels sur les VLAN et IEEE 802.1Q	8
Le serveur d'authentification	11
Les postes clients	12

CHAPITRE 3

Critères d'authentification	15
Authentifier : quoi ?	15
Authentifier : avec quoi ?	16

CHAPITRE 4

Principes des protocoles Radius et 802.1X	19
Principe de l'authentification Radius-MAC	19
Principe de l'authentification 802.1X (EAP)	21

CHAPITRE 5

Description du protocole Radius	25
Origines	25
Format général des paquets	26

Les attributs	28
Les attributs « vendor »	30
Dictionnaires d'attributs	31
Les différents types de paquets	31

CHAPITRE 6

Les extensions du protocole Radius..... 33

Les réseaux virtuels (VLAN)	33
Le support de IEEE 802.1X et EAP	34
Les couches EAP	35
Étape « Identité externe »	36
Étape « Négociation de protocole »	38
Étape « Protocole transporté »	39
Étape « Gestion des clés de chiffrement »	39
Le protocole EAP/TLS	39
Le protocole EAP/PEAP	42
Le protocole EAP/TTLS	46
Spécificités Wi-Fi : la gestion des clés de chiffrement et WPA	50
Historique	50
Transition entre l'authentification et le chiffrement de données	51
TKIP et CCMP	53
En résumé...	54

CHAPITRE 7

FreeRadius..... 55

Installation et démarrage	56
Principes généraux	57
Soumission d'une requête	58
Recherche dans la base de données	58
Constitution de la liste des autorisations	59
Authentification	59
Config-items	59
Les principaux fichiers de configuration	60
Clients.conf	61
La base users	61
<i>Format</i>	62
<i>Les opérateurs</i>	62
<i>DEFAULT et Fall-Through</i>	64
Radiusd.conf	65
<i>Paramètres du service Radiusd</i>	65

<i>Déclaration des modules</i>	66
<i>Section Instantiate</i>	66
<i>Section Authorize</i>	66
<i>Section Authenticate</i>	67
<i>Les autres sections</i>	67
Le fichier eap.conf	68
<i>Configuration du module tls</i>	68
<i>Configuration du module peap</i>	71
<i>Configuration du module ttls</i>	74
Dictionnaires	74
Les autres fichiers de configuration	75
Proxy.conf	75
<i>Domaine en préfixe</i>	76
<i>Domaine en suffixe</i>	77
Huntgroups	78
Les variables	79
Syntaxe	79
Syntaxe conditionnelle	79
Exécution de programmes externes	80

CHAPITRE 8

Mise en œuvre de FreeRadius 83

Authentification Radius-MAC sur réseau sans fil	84
Mise en œuvre des bornes	84
<i>Connexion de la borne sur un commutateur HP 2626</i>	85
<i>Connexion de la borne sur un commutateur Cisco 2960</i>	85
<i>Configuration d'une borne HP 420</i>	85
<i>Configuration d'une borne Cisco Aironet 1200</i>	89
Configuration du serveur FreeRadius	92
<i>Déclaration des bornes</i>	92
<i>Configuration de radiusd.conf</i>	93
<i>Configuration du fichier users</i>	93
Configuration des postes client	94
Authentification 802.1X sur réseau sans fil	95
Configuration des bornes	95
<i>Connexion des bornes sur des commutateurs HP et CISCO</i>	95
<i>Configuration d'une borne HP 420</i>	95
<i>Configuration d'une borne Cisco Aironet</i>	96
Configuration du serveur FreeRadius	97
<i>Déclaration des bornes dans clients.conf</i>	97
<i>Configuration de radiusd.conf</i>	98

<i>Configuration de eap.conf</i>	98
<i>Configuration de users</i>	99
Authentification Radius-MAC sur réseau filaire	101
Mise en œuvre des commutateurs	101
<i>Configuration d'un commutateur HP 2626</i>	101
<i>Configuration d'un commutateur Cisco 2960</i>	102
Configuration du serveur FreeRadius	102
Configuration des postes client	103
Authentification 802.1X sur réseau filaire	103
Configuration d'un commutateur HP 2626	103
Configuration d'un commutateur Cisco 2960	103
Mise en œuvre des certificats	104
Format des certificats	105
Plusieurs autorités de certification et listes de révocation	105
Création d'une IGC	107
<i>Création du certificat de l'autorité</i>	107
<i>Création d'un certificat utilisateur ou machine</i>	108

CHAPITRE 9

Configuration des clients 802.1X 111

Clients Windows	111
Installation des certificats	112
Accéder à la configuration du supplicanant	115
Authentification TLS	116
Authentification PEAP	118
Authentification au démarrage	119
<i>Mise en œuvre</i>	119
<i>Installation d'un certificat machine</i>	122
Clients Linux	122
Installation de NDISWRAPPER	123
Installation de wpa_supplicant	124
Installation de Xsupplicant	124
Configuration de wpa_supplicant pour réseau sans fil	125
<i>Configuration pour TLS</i>	126
<i>Configuration pour PEAP</i>	127
<i>Configuration TTLS</i>	128
Configuration de Xsupplicant pour réseau filaire	129
<i>Configuration pour TLS</i>	130
<i>Configuration pour PEAP</i>	131
<i>Configuration pour TTLS</i>	132

CHAPITRE 10

Mise en œuvre des bases de données externes..... 133

Domaine Windows	133
Configuration de Samba	134
Intégration dans un domaine Windows	135
Configuration dans radiusd.conf	136
Base LDAP	136
Rappels sur LDAP	137
Schéma Radius	138
Mécanismes d'interrogation de la base LDAP	139
Configurer LDAP dans radiusd.conf	140
Exemple pour Radius-MAC	142
Exemple pour TLS	143
Exemple pour PEAP	143
Exemple avec TTLS	146
<i>TTLS avec MS-CHAPv2</i>	146
<i>TTLS avec CHAP</i>	147
Prise en compte des check-items	148

CHAPITRE 11

Outils d'analyse 151

Analyse sur le serveur FreeRadius	152
Utilisation de tcpdump	152
Mode debug	153
Analyse sur une borne Cisco Aironet 1200	160
Analyse sur le poste de travail	162

CHAPITRE A

Références..... 165

CHAPITRE B

La RFC 2865 – RADIUS..... 167**Index..... 207**