Étude et mise en œuvre du protocole 802.1X dans le cadre de la politique de sécurité de Sphéria Val de France

Denis Bertrand

CONSERVATOIRE NATIONAL DES ARTS ET METIERS

CENTRE RÉGIONAL ASSOCIÉ D'ORLEANS

MEMOIRE

présenté en vue d'obtenir

le DIPLOME D'INGENIEUR CNAM

SPECIALITE : Informatique

OPTION : Ingénierie des Systèmes d'Information

par

Denis BERTRAND

ETUDE ET MISE EN ŒUVRE DU PROTOCOLE 802.1X DANS LE CADRE DE LA POLITIQUE DE SECURITE DE SPHERIA VAL DE FRANCE

Soutenu le 4 décembre 2013

JURY

PRESIDENT : **M. Fouad BADRAN – Professeur des Universités**

MEMBRES : **M. Jean-Claude PIRKNER**

M. François-Xavier RAYMOND

M. Laurent LOPEZ

Remerciements

Je tiens tout d'abord à remercier le groupe Sphéria Val de France pour m'avoir permis de réaliser ce mémoire dans de très bonnes conditions de travail.

Je remercie également Patrick LEON et Lionel PHILIPPE, mes responsables actuels au sein du GIE SIHM, pour le temps qu'ils m'ont accordé pour la rédaction de ce mémoire.

Je remercie le Conservatoire National des Arts et Métiers d'Orléans, dont l'enseignement m'a beaucoup apporté, professionnellement et personnellement.

Je remercie Laurent LOPEZ, mon responsable au sein de Sphéria Val de France, pour sa disponibilité et ses conseils tout au long de ce projet.

Je remercie Jean-Michel BOISHUS, Arnaud LUISIN, Yann DANO, Gönül MOUTIEE, Fabrice TROISPOUX, Armel COUETTE, mes collègues du Département Informatique Sphéria Val de France, pour leur disponibilité et leur concours durant ce projet.

Je remercie Emmanuel FERRARI, de la société Telindus ainsi que Jamel SEMEH, Consultant Cisco, pour leur aide précieuse, technique et théorique.

Je remercie Jean-Claude PIRKNER, mon tuteur CNAM, pour son suivi, son écoute et ses remarques très judicieuses lors de la réalisation de ce mémoire.

Enfin je remercie ma compagne Nathalie, ma famille et mes proches pour leurs encouragements et leur soutien tout au long de ces années.

Index

802.11, 6

802.1d, 6, 41

802.3, 6

AAA, 6, 50

ACL, 6, 69, 71, 85, 107, 109

ACS, 6, 32, 58, 63, 71, 72, 76, 77, 78, 79, 80, 93, 94, 100, 107, 108, 110, 113, 114, 123

Active Directory, 6

Adresse MAC, 6, 49, 52, 53, 65, 67, 70, 71, 72, 75, 93, 104, 105, 108, 116, 125

ARP, 6, 27, 28

Authentication Server, 6, 33

Authenticator, 6, 33, 40

Call server, 6

CSI, 6, 15, 95, 96, 97

DI, 6, 58, 59, 82, 91, 92, 93, 94, 95, 96, 97

DMZ, 6, 23, 24, 31

Draft, 6

EAP, 6, 33, 34, 35, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 55, 62, 63, 64, 65, 66, 67, 70, 71, 72, 74, 76, 90, 93, 100, 101, 108, 132

EAPOL, 6, 34, 35, 37, 41, 42, 107

GPO, 6, 80, 92, 97, 99, 100, 121

GTB, 6, 57, 65, 67, 68, 71, 80

Hash, 6

IEEE, 6, 40, 90, 101, 126, 127

IETF, 6, 47, 50, 127

IP, 6, 14, 17, 18, 26, 27, 28, 32, 55, 57, 58, 63, 64, 65, 66, 67, 68, 70, 71, 74, 75, 77, 80, 92, 106

IP spoofing, 6, 27

ITIL, 6, 15, 17

LDAP, 6, 7, 50, 90

MAB, 7, 108, 112

MAC, 27, 49

MPLS, 7, 18

OU, 7

PAC, 7, 48

PAE, 7, 33, 34

Pare-feu, 7, 22

PEAP, 7, 45, 46, 47, 49, 63, 64, 66, 67, 70, 71, 72, 74, 90, 93, 101, 102, 108, 112

PKI, 7, 31, 44

PRA, 7, 18, 29, 85

RADIUS, 7, 31, 33, 35, 36, 46, 47, 50, 51, 52, 53, 54, 55, 58, 63, 64, 72, 74, 78, 79, 85, 87, 93, 97, 107, 118, 119, 126, 132

RFC, 7, 43, 50, 56, 90

SIP, 7, 18

SIT, 7, 15, 91, 92, 93, 94, 95, 96, 97

Spanning-tree, 7

Supplicant, 7, 33, 36, 37, 38, 39, 40, 41, 43, 44, 45, 53

SVF, 7, 13, 18, 20, 21, 33, 56, 57, 58, 59, 60, 61, 63, 64, 66, 67, 71, 74, 76, 77, 80, 82, 87, 91, 92, 93, 94, 98, 99, 103, 114, 120, 122, 124, 125

TCP, 7, 28
TLS, 7, 44, 45, 46, 47, 63, 64, 66, 67, 70, 71, 72, 74, 76, 90, 93, 100, 108
VABF, 7, 94
VLAN, 7, 67, 68, 69, 70, 71, 82, 93, 107, 109
VSR, 7
VSS, 7, 31
WAN, 7, 18
WEP, 7, 44, 47

Glossaire

802.11 : Spécifications pour l'implémentation de réseaux locaux à liaison sans fil.

802.1d : Spécifications du protocole Spanning-tree.

802.3 : Spécifications pour l'implémentation de réseaux locaux à liaison filaire.

AAA : Authentication, Authorization and Accounting.

ACL : Access Control List

ACS : Access Control Server.

ARP : Address Resolution Protocol.

Active Directory : Implémentation par Microsoft des services d'annuaire LDAP pour les systèmes d'exploitation Windows.

Adresse MAC : Media Access Control ou contrôle d'accès au support. Information physique unique stockée dans une carte réseau ou une interface réseau.

Authenticator : Equipement authentificateur.

Authentication Server : Serveur d'authentification.

Call server : Autocommutateur téléphonique IP.

CSI : Centre de Service Informatique.

DI : Département Informatique.

DMZ : Demilitarized zone.

Draft : Proposition de document.

EAP : Extensible Authentication Protocol.

EAPOL : Extensible Authentication Protocol Over LAN.

GPO : Groupe Policy Object.

GTB : Gestion Technique du Bâtiment.

Hash : Somme de contrôle, empreinte.

IEEE : Institute of Electrical and Electronics.

IEEE 802 : Comité de l'IEEE en charge des normes relatives aux réseaux locaux et métropolitains.

IETF : Internet Engineering Task Force.

IP : Internet Protocol.

IP spoofing : Usurpation d'adresse IP.

ITIL : Information Technology Infrastructure Library.

LDAP : Lightweight Directory Access Protocol.

MAB : Mac Authentication Bypass.

MPLS : MultiProtocol Label Switching.

OU : Organization Unit.

PAC : Protected Access Credential.

PAE : Port Access Entity.

Pare-feu : équipement de sécurité permettant de filtrer les accès aux ressources réseaux.

PEAP : Protected Extensible Authentication Protocol.

PKI : Public Key Infrastructure.

PRA : Plan de Reprise d'Activité.

RADIUS : Remote Authentication Dial-In User.

RFC : Request For Comments.

SIP : Session Initiation Protocol.

SIT : Service Infrastructure Technique.

Spanning-tree : Protocole réseau de niveau 2 permettant de déterminer une topologie réseau sans boucle.

Supplicant : Equipement à authentifier.

SVF : Sphéria Val de France.

TCP : Transmission Control Protocol.

TLS : Transport Layer Security.

VABF : Vérification d'Aptitude Au Bon Fonctionnement.

VLAN : Virtual Local Area Network.

VSR : Vérification de Service Régulier.

VSS : Virtual Switching System.

WAN : Wide Area Network.

WEP : Wired Equivalent Privacy.

Table des matières

REMERCIEMENTS **3**
INDEX **4**
GLOSSAIRE **6**
INTRODUCTION **12**
1. PRESENTATION DE SPHERIA VAL DE FRANCE **13**
1.1. Présentation du Département Informatique ***14***
1.2. Organisation du Département Informatique ***15***
1.3. Poste occupé ***15***
2. CONTEXTE DU PROJET **16**
2.1. Contexte économique ***16***
2.2. Contexte réglementaire ***16***
2.3. Contexte qualité ***17***
2.4. Contexte technique et fonctionnel : le SI existant ***17***
3. LES OBJECTIFS DU PROJET **20**
4. ÉTAT DE L'ART DE LA SECURITE DANS LE CADRE DE L'ACCES AU RESEAU D'ENTREPRISE **22**
4.1. La sécurisation des réseaux informatiques ***22***
4.1.1. La prévention des menaces externes 22
4.1.2. La prévention des menaces internes 24
4.2. Méthodologie globale d'intrusion et les différents types d'attaques ***25***
4.2.1. Méthodologie globale d'intrusion 26
4.2.2. Usurpation d'adresse IP (IP spoofing) 27
4.2.1. Attaque du protocole ARP (ARP poisoning) 27
4.2.2. Vol de session TCP (TCP Session Hijacking) 28
4.2.3. Les attaques par déni de service 28
4.3. La nécessité de la sécurisation du réseau local ***29***
5. PRESENTATION DES MOYENS **29**
5.1. Organisation du projet ***29***
5.2. Planning ***30***
5.3. Budget ***31***

5.4. Infrastructure en place 31

6. LE PROTOCOLE 802.1X 33

6.1. Principe général du protocole 802.1x 33

6.2. Le point d'accès au réseau : PAE 34

6.3. Fonctionnement du protocole 802.1x 35

6.3.1. Scénario 1 : Processus de base 36

6.3.2. Scénario 2 : Supplicant non configuré 36

6.3.3. Scénario 3 : Pas d'authentificateur 37

6.3.4. Scénario 4 : Pas de serveur d'authentification 37

7. LE PROTOCOLE EAP 38

7.1. Extensible Authentication Protocol (EAP) 39

7.2. Extensible Authentication Protocol Over LAN (EAPOL) 41

7.3. Les méthodes EAP ou EAP-Methods 42

7.3.1. EAP-MD5 43

7.3.2. EAP-TLS (Tunneled Transport Layer Security) 44

7.3.3. EAP-MS-CHAPV2 45

7.3.4. EAP-PEAP (Protected EAP) 45

7.3.5. EAP-TTLS (Tunneled TLS) 46

7.3.6. LEAP (Lightweight Extensible Authentication Protocol) 47

7.3.7. EAP-FAST (Flexible Authentication via Secure Tunneling) 47

7.4. Les failles du protocole EAP 48

7.4.1. Attaque par dictionnaire hors-ligne 48

7.4.2. Attaque par dictionnaire en ligne 49

7.4.3. Attaque de la session 49

7.4.4. Attaques MIM (Man in the Middle) 50

8. LE PROTOCOLE RADIUS 50

8.1. Principe de l'authentification RADIUS-MAC 52

8.2. Principe de l'authentification 802.1x 53

8.3. Description du protocole RADIUS 54

8.3.1. Les types de paquets RADIUS 54

8.3.2. Les attributs RADIUS 55

8.4. Synthèse 56

9. LE PROTOCOLE 802.1X DANS LE CONTEXTE DE SVF 56

9.1. Les composants de l'architecture 802.1x chez SVF 57
9.1.1. Les systèmes SVF à authentifier 57
9.1.2. Les systèmes authentificateurs SVF 58
9.1.3. Le serveur d'authentification SVF 58
9.2. Les différents types de clients 58
9.3. Périmètre géographique de déploiement du 802.1x 62
10. ETUDE DES METHODES D'AUTHENTIFICATION POSSIBLES 62
10.1. Les systèmes EAP de SVF à authentifier 63
10.2. Les systèmes EAP authentificateurs de SVF 63
10.3. Le serveur d'authentification SVF 63
10.4. Le serveur d'annuaire SVF 64
10.5. Récapitulatif des méthodes EAP par système 64
11. CHOIX DES METHODES D'AUTHENTIFICATION 65
11.1. Les méthodes d'authentification pour les équipements non 802.1x 65
11.2. Les méthodes d'authentification pour les équipements 802.1x 66
11.3. Récapitulatif des méthodes d'authentification retenues 67
12. UTILISATION DE VLAN SPECIFIQUES 67
13. UTILISATION D'ACCESS CONTROL LIST (ACL) 69
14. PRESENTATION ET MISE EN PLACE DE LA MAQUETTE 70
14.1. Description de la maquette 70
14.2. Paramétrage des systèmes authentificateurs 71
14.3. Paramétrage du serveur d'annuaire 72
14.4. Paramétrage du serveur RADIUS 72
14.5. Paramétrage du serveur de certificat 73
14.6. Paramétrage des systèmes à authentifier 74
14.6.1. Paramétrage des ordinateurs SVF 74
14.6.2. Paramétrage des ordinateurs Prestataires 74
14.6.3. Paramétrage des téléphones IP 74
14.7. Phase de tests 75
14.7.1. Résultats des tests 75
14.7.2. Modifications apportées suite aux tests 77
14.8. Bilan de la phase de maquettage 79
15. DEPLOIEMENT 79

15.1. Préparation du déploiement ... *80*
15.1.1. Procédure de migration ... 81
15.1.2. Procédure d'installation d'un nouvel équipement ... 81
15.2. Déploiement sur un périmètre restreint ... *82*
15.3. Déploiement sur le périmètre global ... *82*
15.3.1. Première étape ... 83
15.3.2. Seconde étape ... 84
16. BILAN ... **84**
17. PERSPECTIVES D'EVOLUTION ... **85**
17.1. Déploiement sur de nouveaux sites du groupe ... *85*
17.2. Renforcement de la sécurité ... *85*
17.3. Sécurisation de l'accès internet ... *85*
CONCLUSION ... **87**
TABLE DES ANNEXES ... **89**
REFERENCES ... **126**
LISTE DES FIGURES ... **128**

Introduction

Suite au déménagement de son siège social en avril 2010 dans de nouveaux locaux qui a nécessité la refonte de l'infrastructure réseau, la Direction du groupe Sphéria Val de France a souhaité améliorer la sécurisation de son SI en mettant en place une politique de sécurité.

Différentes actions ont alors été menées avec notamment la formalisation de la gestion des données informatiques dans le cadre d'un changement de matériel, la gestion des droits et habilitations par la mise en place de procédures, les stratégies concernant les comptes et mots de passe, la journalisation des évènements, la mise en place d'un processus de gestion des incidents de sécurité.
A cela s'ajoute une charte informatique remise à chaque salarié indiquant ses responsabilités dans l'utilisation de l'accès à internet, de la messagerie et du matériel mis à sa disposition par l'entreprise.
Cependant à ce jour rien ne permettait à l'entreprise d'être assurée de l'identité des ordinateurs accédant à son Système d'Information et d'autant plus que l'ensemble des prises réseaux du bâtiment sont pré-câblées et qu'un nombre important de prestataires externes est amené à intervenir régulièrement.

Afin de répondre à cette problématique je vais tout d'abord vous présenter le groupe Sphéria Val de France, puis un état de l'art de la sécurité dans le cadre de l'accès aux réseaux informatiques d'entreprise.
Cela nous amènera à étudier les solutions permettant de répondre à la problématique d'abord d'un point vue théorique puis dans le cadre d'une maquette afin de réaliser des tests et de choisir une solution adaptée à l'environnement et aux contraintes de Sphéria Val de France.
Cette maquette permettra également de préparer le déploiement en production de la solution retenue, d'abord sur un périmètre restreint, puis, après validation, sur le périmètre global.

A chaque étape importante, une réunion regroupant les acteurs du projet sera organisée afin de présenter l'état d'avancement des différents travaux, de répondre aux interrogations et d'arbitrer sur les choix possibles.

1. Présentation de Sphéria Val de France

Sphéria Val de France (SVF) est un groupe mutualiste de santé qui est la fusion de trois mutuelles historiques (Loiret, Eure et Loir, Nièvre). L'entreprise est la première mutuelle en région Centre-Bourgogne. Présente depuis 2005 en région parisienne, elle protège plus de 213 000 adhérents en complémentaire santé.

L'expertise du groupe s'étend de la protection sociale (complémentaire santé, prévoyance, prévention, assistance, épargne-retraite) à la prise en charge médico-sociale de la personne et contribue à faire de Sphéria Val de France un acteur majeur de santé interrégional.
De plus le groupe est certifié ISO 9001.

Quelques chiffres clés :
Le groupe SVF c'est :

- 684 salariés
- 3 sites majeurs : Orléans, Lucé et Nevers
- 21 agences implantées sur 5 départements : le Loiret, l'Eure et Loir, la Nièvre, les Yvelines et l'Essonne
- 125,2 millions d'euros de chiffre d'affaires
- 94,5 millions d'euros de prestations versées

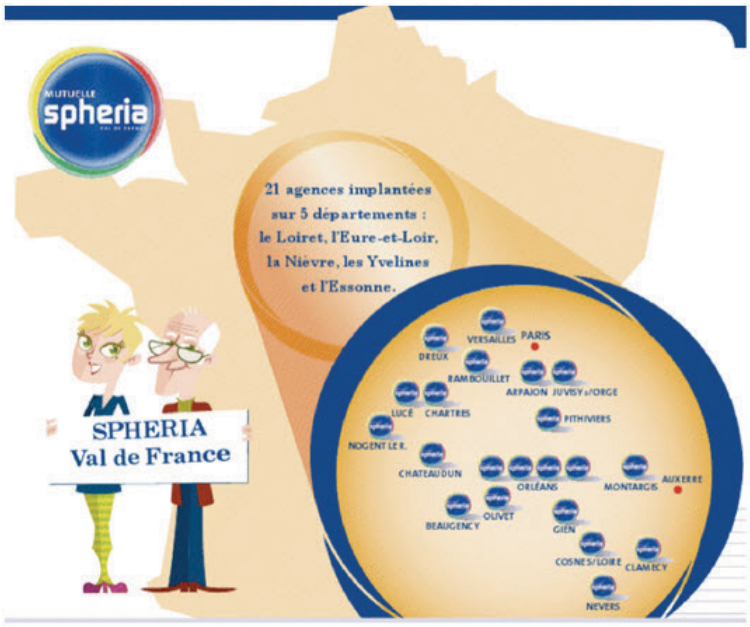


Figure 1: Présentation de Sphéria Val de France.

1.1. Présentation du Département Informatique

Le Département Informatique est chargé de mettre à disposition des utilisateurs, des ressources informatiques, téléphoniques et de visioconférences communes.
Il offre une assistance personnalisée aux utilisateurs, est chargé de maintenir et de faire évoluer le système d'information et est garant de sa sécurité.

Ses missions sont :

- assurer l'assistance des utilisateurs dans le cadre des conventions de services négociées,
- administrer, exploiter et faire évoluer les infrastructures techniques pour l'ensemble des sites du groupe,
- maintenir le parc informatique, planifier les interventions d'installation, de configuration et de dépannage de matériels mis à la disposition des utilisateurs,
- gérer le réseau informatique et faire évoluer l'infrastructure matérielle dans tous les bâtiments,
- administrer et gérer les serveurs d'annuaires du groupe,
- gérer les équipements de téléphonie et les systèmes de visioconférence (IP et RNIS),
- mettre en place les mécanismes concernant la sécurité informatique,
- mettre en place la politique de sauvegarde,
- piloter les projets d'évolution du système d'information.

1.2. Organisation du Département Informatique

Le Département Informatique est composé de 3 services :

- le Centre de Service Informatique (CSI) qui assure le support des utilisateurs,
- le Service Infrastructure Technique (SIT) qui administre et fait évoluer les environnements techniques,
- le Service Projet qui pilote les projets d'évolution du système d'information.

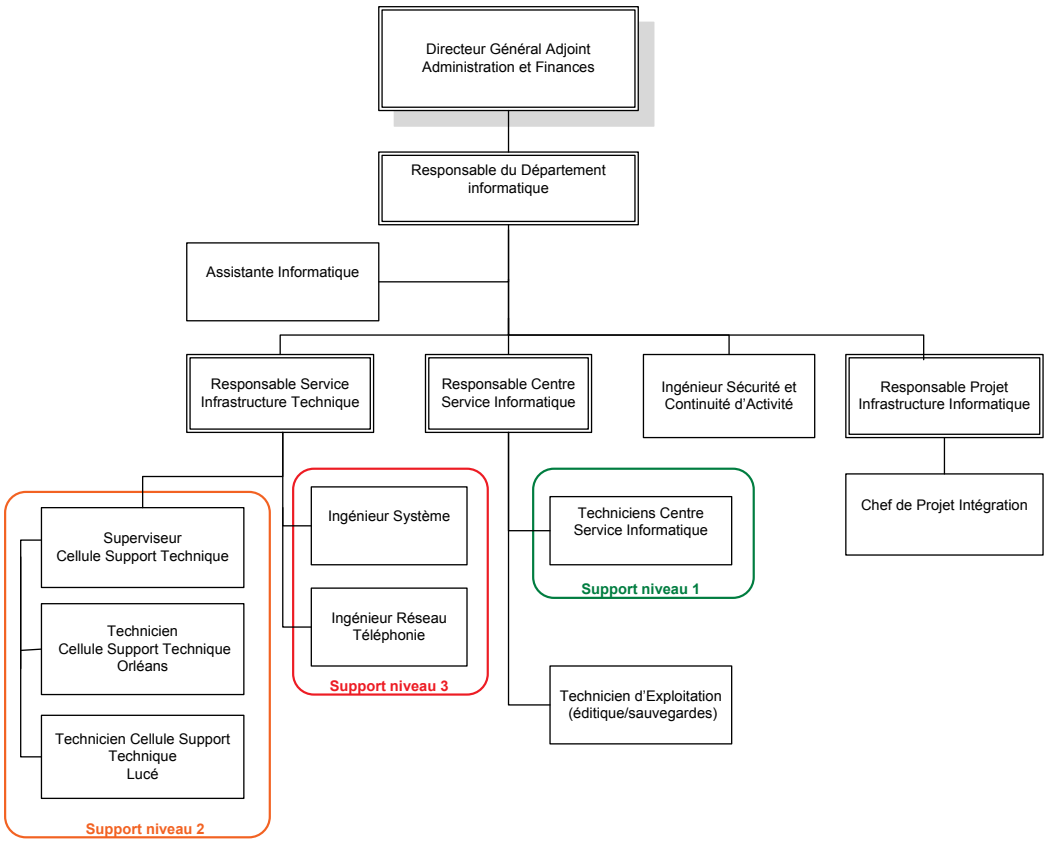


Figure 2: Organigramme du Département Informatique

Depuis 2006 le Département Informatique s'est structuré conformément au référentiel ITIL.

1.3. Poste occupé

De janvier 2008 à février 2012 j'ai occupé le poste d'ingénieur Réseau et Téléphonie au sein de ce département.

A ce titre :

- J'administrais, veillais au bon fonctionnement et à la sécurité de l'infrastructure réseau et téléphonie,
- Je traitais les demandes de services et les incidents de niveau 3,
- Je participais à la mise en œuvre des solutions techniques en mode projet.

J'assurais également ponctuellement le remplacement de l'ingénieur Système.

2. Contexte du projet

2.1. Contexte économique

Apparu en France dans les années 1830-1840[1], le mouvement mutualiste est à l'origine des bases de l'assurance maladie que sont la mise en commun par les adhérents d'une épargne versée sous forme de cotisation et la redistribution des prestations en cas d'impossibilité temporaire de travailler.

Depuis trois décennies, les mutuelles santé doivent compenser le désengagement continu de l'État du régime obligatoire afin que leurs adhérents ne soient pas trop pénalisés mais cette crise de la Sécurité sociale a également eu pour effet d'éveiller l'intérêt des assureurs commerciaux, puis des bancassurances, pour la complémentaire santé, domaine dans lequel les mutuelles se trouvaient en position de monopole jusqu'à la fin des années 1970. Les mutuelles ressentent d'autant plus durement cette concurrence qu'elles se doivent de ne pas sélectionner les adhérents en fonction de leur âge et de leur état de santé.

2.2. Contexte réglementaire

La refonte du Code de la mutualité en 2001 a entériné l'adaptation des mutuelles françaises à la réglementation européenne. Ainsi elles ont dû séparer dans leur gestion les activités d'assurance, dont la complémentaire santé, de celles des réalisations sanitaires et sociales. Le mouvement compte aujourd'hui quelque 2 400 services de soins et d'accompagnement mutualistes (SSAM) et établissements, qui se déclinent en centres d'optique, dentaires, d'audition, cliniques, ...

[1] TOUCAS-TRUYEN P., 2011. Les mutuelles à un tournant – Les corps intermédiaires en perspective

L'entrée en vigueur en 2013 de la réforme européenne Solvabilité II se traduira par un nouveau durcissement des normes prudentielles, obligeant les mutuelles à accumuler des réserves qu'elles estiment inadaptées à leur mode de fonctionnement.
Afin de faire face à ces contraintes, les mutuelles se sont engagées dans un vaste programme de restructuration avec la mise en place d'unions régionales et la disparition progressive des unions départementales. D'un point de vue économique, cette stratégie de regroupement vise à renforcer les moyens techniques et financiers de la mutualité afin de répondre aux défis imposés par la législation européenne et les mesures gouvernementales de baisse du régime obligatoire. L'adoption d'un statut de la mutuelle européenne, réclamé depuis plus de dix ans par la Fédération Nationale de la Mutualité Française, serait une reconnaissance des particularités des organismes mutualistes par rapport aux sociétés de capitaux.

2.3. Contexte qualité

Sphéria Val de France a obtenu en mai 2007, de l'AFAQ AFNOR, la certification ISO 9001 - version 2000. Ce projet initié en début d'année 2006 vise à garantir et à pérenniser des prestations d'un niveau d'exigence élevé, à fidéliser et sécuriser les adhérents actuels et à conquérir de nouveaux marchés. L'obtention de la certification constitue une étape importante dans la recherche d'une qualité de service optimale pour ses adhérents.
Dans le cadre de cette démarche qualité, le Département Informatique de Sphéria Val de France a également adopté les bonnes pratiques ITIL en 2006 avec la mise en place du référentiel ITIL, la création du Centre de Services Informatique (point d'entrée unique de toute demande) et la mise en place de contrats de services.

2.4. Contexte technique et fonctionnel : le SI existant

Tout d'abord il est important de noter que le réseau de l'entreprise est multiservice, il véhicule des flux :

- De données,
- De téléphonie sur IP,
- De visioconférences sur IP.

L'architecture technique du SI de Sphéria Val de France comprend 96 serveurs dont 60 sont virtualisés sur une plateforme WMware. Les serveurs sont reliés à un réseau de stockage SAN et répartis dans deux salles informatiques sur le site Jaurès à Orléans.
Le SI est composé de 165 progiciels dont 90% sont mis à disposition des utilisateurs par l'intermédiaire d'une infrastructure Citrix XenApp.

L'infrastructure comprend également un PABX IP permettant de gérer le centre d'appel et l'ensemble des communications de l'entreprise avec deux Call Server sur le site central, un Call Server passif sur chaque centre de gestion (Lucé, Nevers) et un Call Server passif sur le site de PRA. Le service de fax fonctionne également sur IP avec un lien SIP.

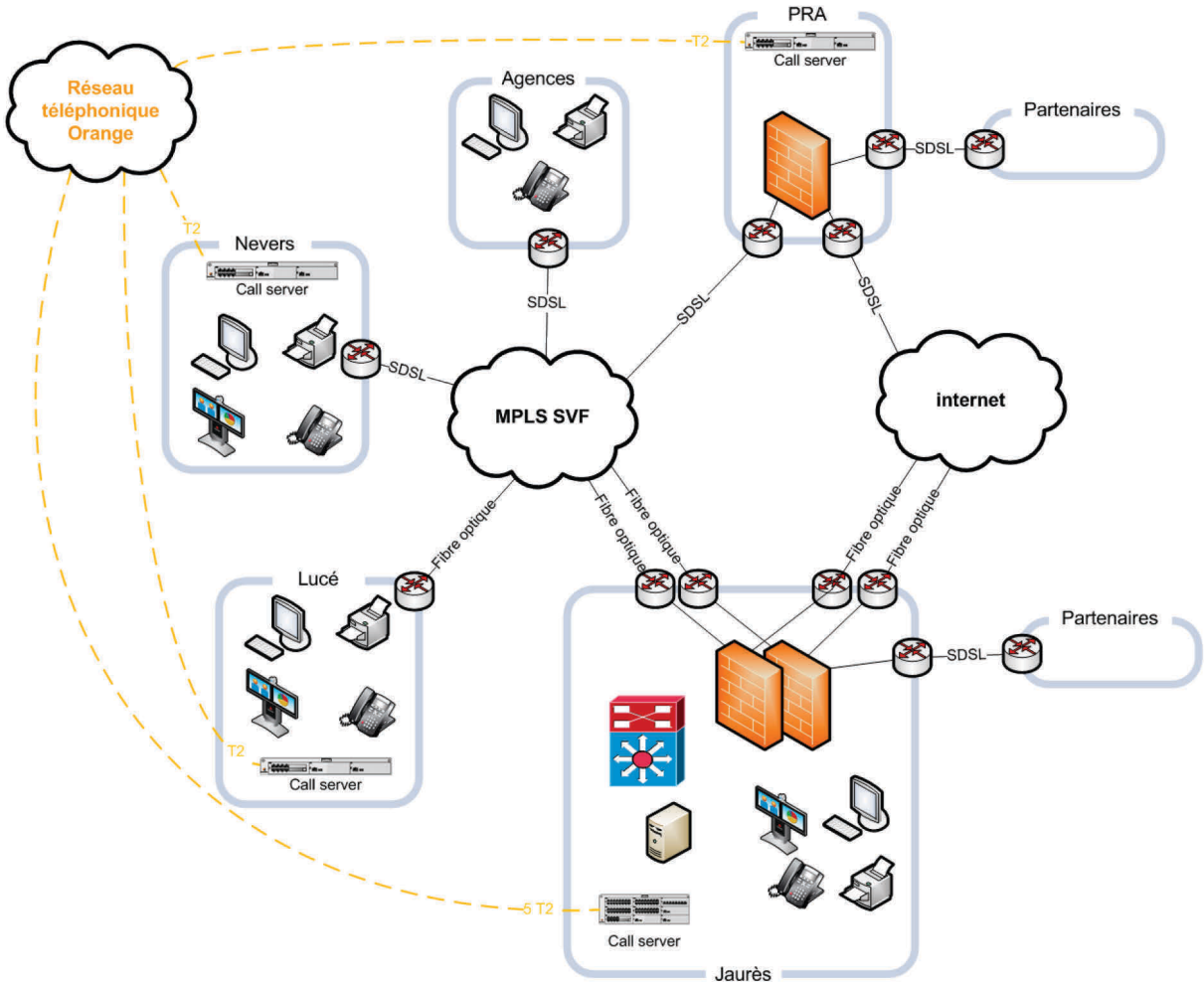


Figure 3: Le réseau global de SVF.

Le réseau WAN de Sphéria Val de France s'appuie sur un réseau MPLS opéré par SFR et relie 23 sites (dont 21 agences et un site de PRA).

Le cœur de réseau utilise la technologie Cisco Virtual Switching System qui permet de créer un commutateur logique à partir des deux châssis physiques répartis dans les deux salles informatiques. Cette technologie permet de s'affranchir de la gestion des boucles de spanning-tree entre les commutateurs de cœur et les commutateurs de distribution. Elle permet de simplifier l'architecture et l'exploitation.

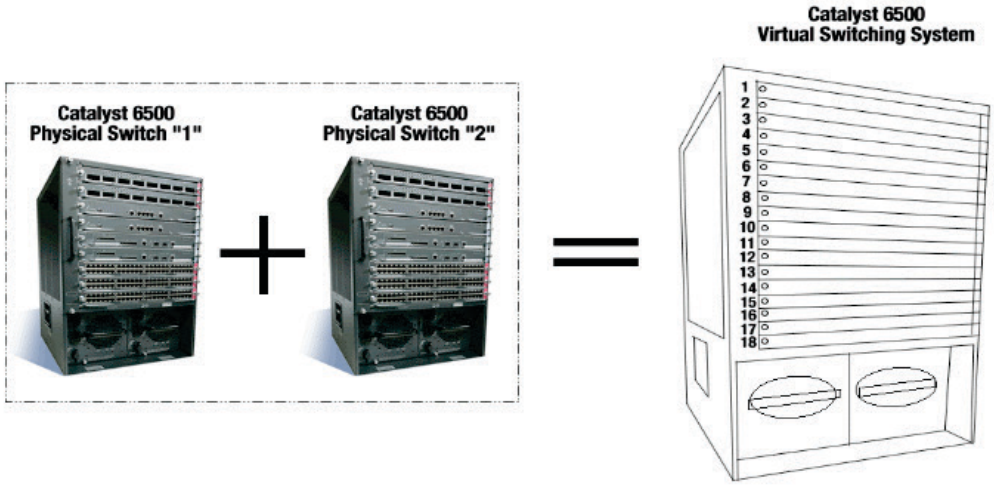


Figure 4: Technologie Cisco Virtual Switching System.

Les six étages du bâtiment sont alimentés par des piles de commutateurs doubles attachés au cœur de réseau par des liaisons fibres à 10 gigabits.

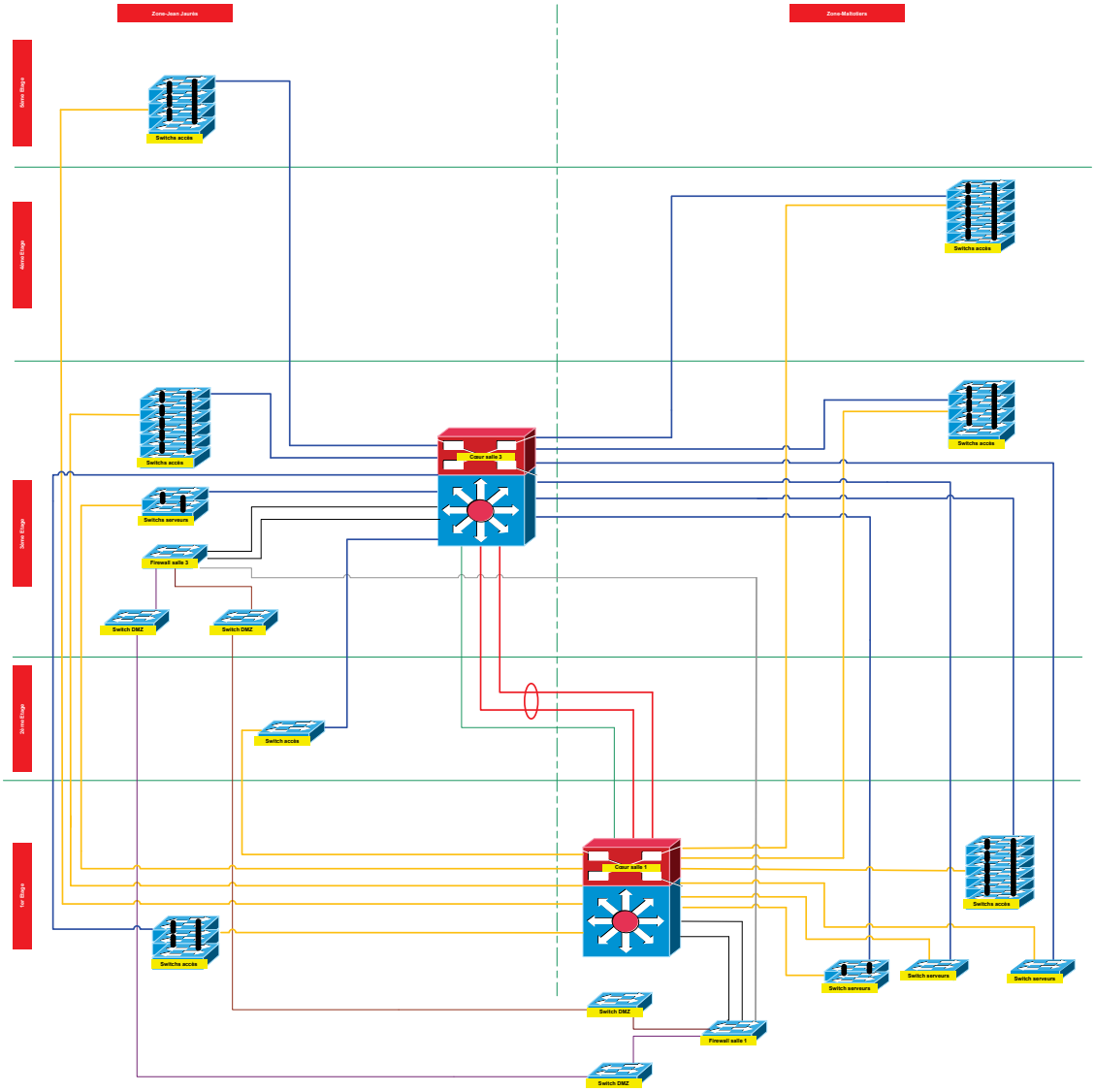


Figure 5: Architecture réseau du siège social de SVF.

3. Les objectifs du projet

La solution technique retenue, doit sécuriser l'accès au réseau local du site Jaurès en répondant à un certains nombres de critères :

- Donner accès au réseau aux équipements de l'entreprise,
- Donner un accès restreint aux machines extérieures nécessitant d'être autorisées,
- Bloquer et empêcher toute tentative de connexion d'un équipement non autorisé.

Le diagramme ci-dessous, défini par l'équipe projet, décrit le processus d'authentification qui devra être suivi :

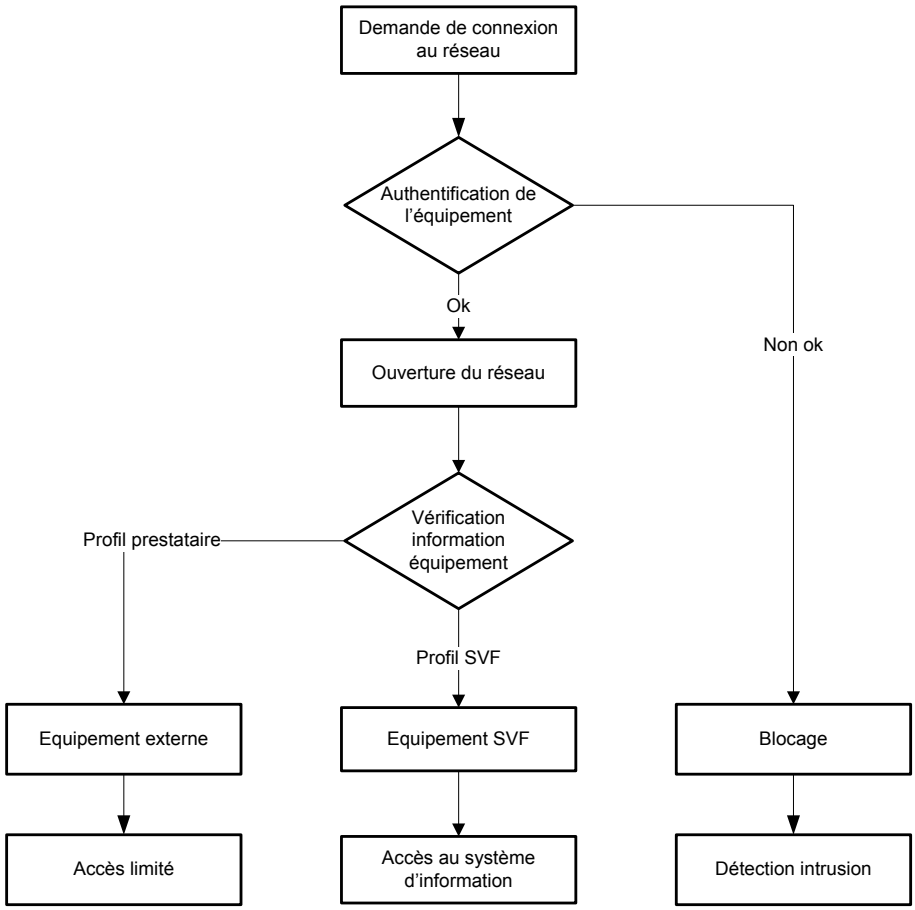


Figure 6: Processus d'authentification.

Le périmètre de ce projet ne couvre que les connexions physiques, la Direction de SVF n'ayant pas souhaité implémenter de réseau wifi.

Mon objectif consiste donc à étudier les protocoles, définir une architecture et mettre en œuvre la meilleure solution répondant aux attentes de Sphéria Val de France en tenant compte de son environnement et de ses contraintes.

4. État de l'art de la sécurité dans le cadre de l'accès au réseau d'entreprise

4.1. La sécurisation des réseaux informatiques

Depuis quelques années, prenant conscience de la prépondérance du système d'information dans leur fonctionnement les entreprises se montrent plus sensibles à la sécurité de leur réseau informatique.

Si au départ le réseau local se trouvait protégé par les murs de l'entreprise, l'apparition des systèmes d'accès distants puis d'internet a radicalement modifié ce fait. Ainsi est apparue la nécessité d'un contrôle accru des accès. A cela s'ajoute désormais le nombre croissant d'entreprises disposant de réseaux Wifi qui augmente le risque d'intrusion.

L'information étant une ressource stratégique pour l'entreprise, sa protection est indispensable car elle permet de :

- Garantir la continuité d'activité de l'entreprise,
- Réduire les dommages éventuels sur l'activité de l'entreprise,
- Maximiser le retour sur investissement des systèmes d'information.

4.1.1. La prévention des menaces externes

Afin de filtrer les échanges entre l'extérieur et l'intérieur des entreprises, celles-ci mettent en œuvre un ou plusieurs firewalls (pare-feu).

Les architectures les plus courantes sont :

- Architecture simple : le pare-feu interconnecte un réseau privé à un réseau public. C'est l'architecture classique en entreprise pour filtrer l'accès à internet.

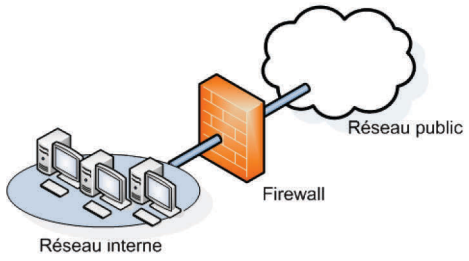


Figure 7: Pare-feu de périmètre.

- Architecture avec une DMZ : le pare-feu est connecté à trois réseaux différents :
    - Le réseau interne de l'entreprise,
    - Un réseau appelé zone démilitarisée ou DMZ,
    - Le réseau public (par exemple Internet).

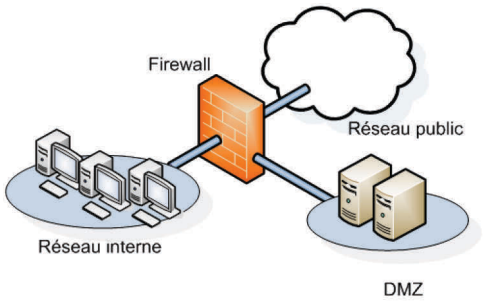


Figure 8: Périmètre en 3 parties.

- Architecture avec pare-feu dos à dos : le pare-feu interne filtre les échanges entre le réseau interne de l'entreprise et la DMZ. Le pare-feu externe, quand à lui, filtre les échanges entre la DMZ et le réseau public.

  L'avantage de cette solution est de configurer des règles plus strictes que sur l'architecture précédente.

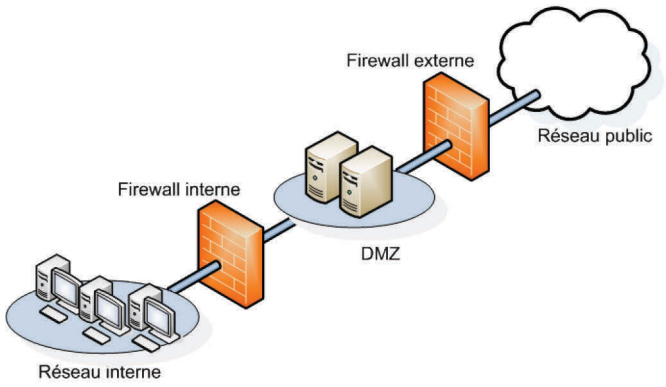


Figure 9: Pare-feux dos à dos.

Avantages et inconvénients des trois solutions :

Tableau I : Comparatif des architectures de firewall.

Architecture	Avantages	Inconvénients
Architecture simple	• Simple • Coût réduit	• Un seul point d'attaque et de faille
Architecture avec une DMZ	• Sécurisation accrue par une séparation des réseaux	• Un seul point d'attaque et de faille
Architecture en trois parties	• Niveau de sécurité encore plus élevé • Règles plus strictes	• Complexification de l'administration • Coût plus élevé

4.1.2. La prévention des menaces internes

Dans la sécurisation d'un système d'information la protection contre les attaques externe n'est pas suffisante, il est également nécessaire de se préoccuper des menaces internes.

Les solutions mises en œuvre dans ce cas précis s'appuient sur :

- La sécurisation du poste de travail en utilisant des méthodes d'authentification sur les machines,
- La sécurisation du réseau local en utilisant des méthodes d'authentification sur les serveurs,
- La sécurisation des applications en utilisant des méthodes d'authentification spécifiques aux logiciels.

Ainsi, la sécurisation du Système d'Information d'une entreprise repose sur des solutions ou des équipements qu'elle-même maîtrise. Malgré tout, il reste la possibilité d'une connexion à partir d'un ordinateur personnel sur le réseau de l'entreprise.
Dans ce cas il faut distinguer deux types d'utilisateurs : ceux qui sont habituellement autorisés à se connecter au réseau et ceux qui ne le sont pas.

4.1.2.1. Les connexions au réseau d'une personne non autorisée

Ces connexions peuvent être réalisées de deux manières :

- La connexion filaire : pour se connecter au réseau informatique il est nécessaire de trouver une prise informatique disponible dans l'entreprise. Et si toutefois cette dernière a veillé à ne pas raccorder ou activer une prise non utilisée, la personne non autorisée aura toujours la possibilité d'utiliser la prise d'un ordinateur non utilisé.

- La connexion sans fil : dans ce cas, il suffit d'être à portée d'une borne wifi pour capter le signal radio et tenter de se connecter au système d'information. Les entreprises maîtrisant souvent mal les ondes radios de leurs bornes il n'est plus nécessaire d'être dans les locaux pour se connecter.

4.1.2.2. Les connexions au réseau d'une personne autorisée

Il s'agit dans ce cas de prestataires ou de clients et la réponse apportée par l'entreprise peut varier selon le degré de maturité vis-à-vis de la sécurité mais bien souvent aucune solution technique n'est proposée. Il est donc obligatoire de mettre à disposition de cette population d'utilisateurs une solution permettant de se connecter au système d'information en assurant la sécurité de celui-ci.

4.2. Méthodologie globale d'intrusion et les différents types d'attaques

Les pirates utilisent généralement la même méthodologie pour s'introduire dans un système informatique. La connaissance de celle-ci, ainsi que des principaux types d'attaques, doit nous permettre de protéger le réseau informatique local en ayant conscience de ses vulnérabilités.

4.2.1. Méthodologie globale d'intrusion

Le schéma ci-dessous[2] décrit la méthodologie la plus fréquemment utilisée pour s'introduire dans un système d'information.

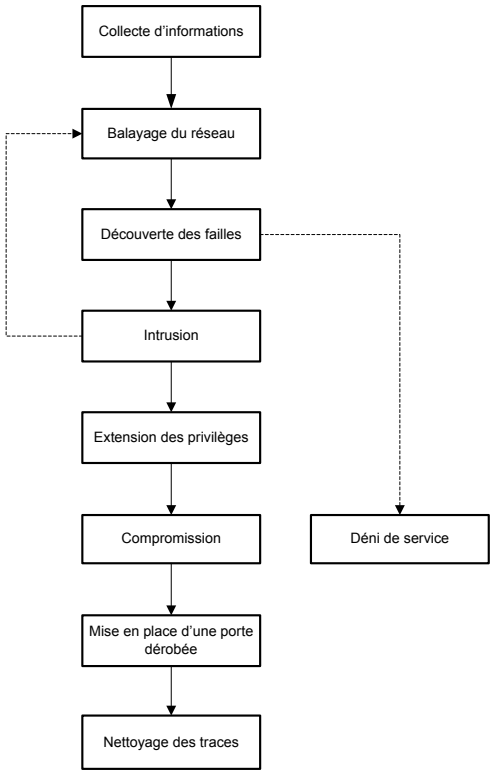


Figure 10: Méthodologie globale d'intrusion.

Collecte d'informations : Il s'agit de récupérer le maximum d'informations concernant le système d'information de l'entreprise : adresses IP, protocoles réseaux, services associés, architecture du réseau, architecture des serveurs, noms de domaine …

Balayage du réseau : Lorsque l'architecture du réseau est connue, le pirate peut le « scanner » à l'aide d'outils fonctionnant :

- En mode actif : des requêtes sont envoyées sur le réseau afin d'obtenir des informations. Cette méthode est détectable par les systèmes de détection d'intrusion,
- En mode passif : cette méthode consiste à simplement écouter les paquets transmis sur le réseau et elle est indétectable.

[2] http://nocremetz.free.fr/ccm/attaques/methodologie.htm

Repérage des failles : Avec les informations ainsi récoltées, le pirate va pouvoir repérer les failles du système d'information en utilisant un scanner de vulnérabilité.

Intrusion : Maintenant que les failles sont repérées, le pirate peut s'introduire sur le réseau.

Extension des privilèges : Une fois introduit sur le réseau, le pirate va chercher à augmenter ses privilèges jusqu'à obtenir les droits « administrateurs ».

Compromission : Désormais, le pirate est en mesure de dresser une cartographie complète du réseau. Il peut alors, en tant qu'« administrateur » d'au moins un ordinateur, étendre ses privilèges sur l'ensemble du réseau par l'intermédiaire des relations d'approbation existant entre les différentes machines.

Porte dérobée : Le pirate va installer une application générant artificiellement une faille de sécurité pour se reconnecter plus tard.

Nettoyage des traces : Le pirate efface les traces de son intrusion (journaux d'évènements, fichiers).

4.2.2. Usurpation d'adresse IP (IP spoofing)

Cette technique consiste à remplacer l'adresse IP d'un paquet émis par une autre adresse IP. Cela permet d'envoyer des paquets anonymement mais également de traverser un pare-feu grâce à une adresse IP valide.
Ainsi le pirate peut cacher la source de son attaque ou profiter d'une relation de confiance entre deux machines.

4.2.1. Attaque du protocole ARP (ARP poisoning)

Cette technique est utilisée pour rediriger le trafic réseau d'une ou plusieurs machines vers la machine du pirate en utilisant une faille du protocole ARP .Celui-ci permet de résoudre une adresse IP en une adresse MAC.

Le pirate va chercher à s'interposer entre deux machines du réseau et transmettre à chacune un paquet ARP falsifié avec sa propre adresse, indiquant que l'adresse de l'autre machine a changé.
Ainsi, à chaque fois que les deux machines souhaiteront communiquer, elles passeront par l'intermédiaire de celle du pirate.

4.2.2. Vol de session TCP (TCP Session Hijacking)

Cette technique est utilisée pour intercepter une session TCP entre deux machines afin de la détourner. Elle peut alors permettre au pirate d'outrepasser une protection par mot de passe, comme lors d'une session telnet ou ftp.

4.2.3. Les attaques par déni de service

La plupart des attaques de ce type s'appuie sur des failles dans l'implémentation d'un protocole du modèle TCP/IP. Il ne s'agit pas ici de récupérer des informations, mais de nuire au bon fonctionnement du système d'information d'une entreprise en le rendant indisponible.

Voici les attaques par déni de service les plus connues :

- Attaque par réflexion (smurf) : cette technique est basée sur l'utilisation de serveurs de diffusion capables de dupliquer un message et de l'envoyer sur toutes les machines pour bloquer le réseau.
- Attaque du ping de la mort (ping of death) : le principe consiste à envoyer sur une machine un datagramme IP d'une taille supérieure à la taille autorisée (65536 octets). Cela entraînera un blocage si la pile TCP/IP de la machine n'est pas protégée contre ce genre d'attaque. Les systèmes récents ne sont plus vulnérables à ce type d'attaque.
- Attaque par fragmentation (fragment attack) : cette attaque s'appuie sur la fragmentation des paquets du protocole IP, il s'agit donc d'insérer dans les paquets fragmentés des informations de décalage erronées. Le récepteur qui rassemble les paquets trouvera des vides ou des recoupements qui bloqueront le système.
- Attaque SYN (TCP/SYN Flooding) : cette attaque consiste à envoyer un grand nombre de requêtes SYN à un hôte avec une adresse IP source inexistante ou invalide. Cette machine cible ne recevra jamais de validation de connexion par paquet ACK.

Même si elle possède un mécanisme d'expiration de connexion en attente, le nombre important de paquets SYN envoyés pourra la bloquer.

4.3. La nécessité de la sécurisation du réseau local

Comme nous l'avons vu, les entreprises sont globalement bien sécurisées du monde extérieur grâce à l'utilisation de firewall. Cependant elles oublient souvent que les menaces sont également internes.

Comme l'indiquait déjà en 2002 Nicolas Six dans son article « Le danger vient de la citadelle informatique »[3], la plupart des problèmes (fuites d'informations, déni de service …) proviennent de l'intérieur de l'entreprise. Une étude de NSC Technology datée de 2001 précisait à ce sujet que seulement 10% des attaques sur les systèmes informatiques d'entreprise étaient dues à des pirates.
Les entreprises ont depuis fait beaucoup d'efforts pour sécuriser les postes de travail, les serveurs et les applications mais il n'est souvent pas prévu de bloquer l'accès au réseau à une personne tentant de se connecter avec une machine non conforme.

5. Présentation des moyens

5.1. Organisation du projet

L'équipe constituée pour mener à bien ce projet se compose :

- Du Responsable du Département Informatique, représentant la Maîtrise d'ouvrage,
- Du Responsable du service Projets,
- Du Responsable Service Infrastructure Technique,
- De l'ingénieur Sécurité et PRA,
- De l'ingénieur Système,
- D'un consultant de la société Telindus,
- Et de moi-même, en qualité de chef de projet.

[3] http://www.journaldunet.com/solutions/0210/021002_secu.shtml

5.2. Planning

Le planning ci-dessous indique les étapes du projet ainsi que les différents jalons.

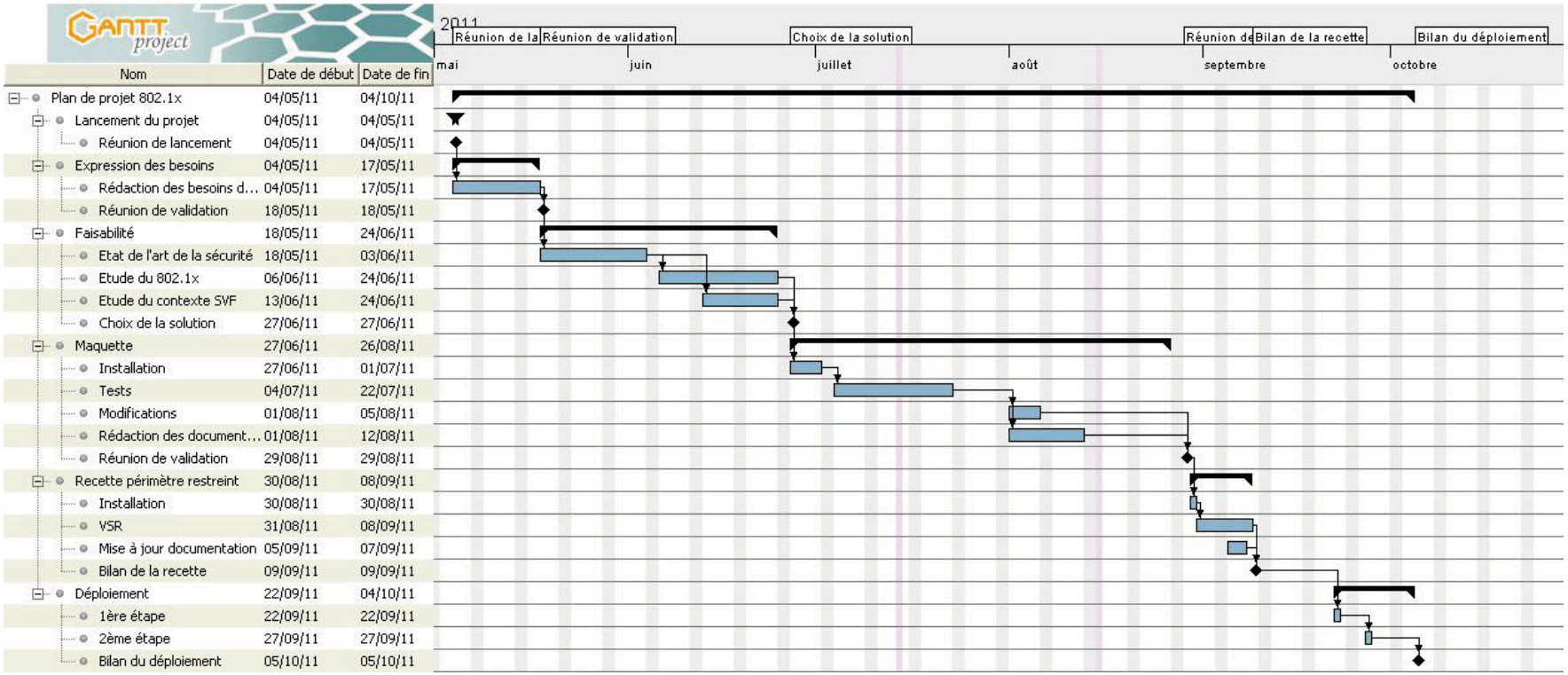


Figure 11: Planning du projet.

5.3. Budget

Les investissements, d'un montant de 12 000 €HT, concernant l'acquisition de serveurs RADIUS ont été réalisés dans le cadre du projet Réseau mené en 2009-2010 pour le déménagement du siège social.

Le serveur PKI utilisé dans ce projet fait déjà partie de l'infrastructure du groupe, il s'agit d'un serveur Windows 2003 Enterprise Edition.

5.4. Infrastructure en place

Nous avons vu que le cœur de réseau de Sphéria Val de France est composé de deux châssis Cisco 6506 répartis dans deux salles informatiques. Fonctionnant en mode VSS (Virtual Switching System) les deux équipements sont considérés et donc administrés comme un seul commutateur logique.

Chaque commutateur ou pile de commutateurs (DMZ, serveurs, accès) est physiquement connecté à chacun des châssis du cœur de réseau.

Un serveur RADIUS est installé dans la salle informatique au premier étage et a le rôle de serveur primaire, sa configuration est répliquée de manière régulière sur le serveur secondaire de la salle informatique du troisième étage. C'est lui qui gère toutes les demandes d'authentification.

Le serveur de certificats sert à la génération des certificats clients et gère la liste de révocation des certificats obsolètes. Le serveur RADIUS contacte le serveur de certificats uniquement pour consulter la liste de révocation, il n'est donc pas indispensable de redonder ce dernier. Une procédure de sauvegarde/restauration s'avère suffisante.

L'infrastructure technique concernée par ce projet se décompose donc ainsi :

- 31 commutateurs Cisco 3750E servant aux accès des utilisateurs et à la connexion des matériels dits périphériques (imprimante, téléphone IP, …),
- 2 serveurs Radius Cisco ACS,
- 1 serveur de certificat,
- L'annuaire Active Directory de l'entreprise.

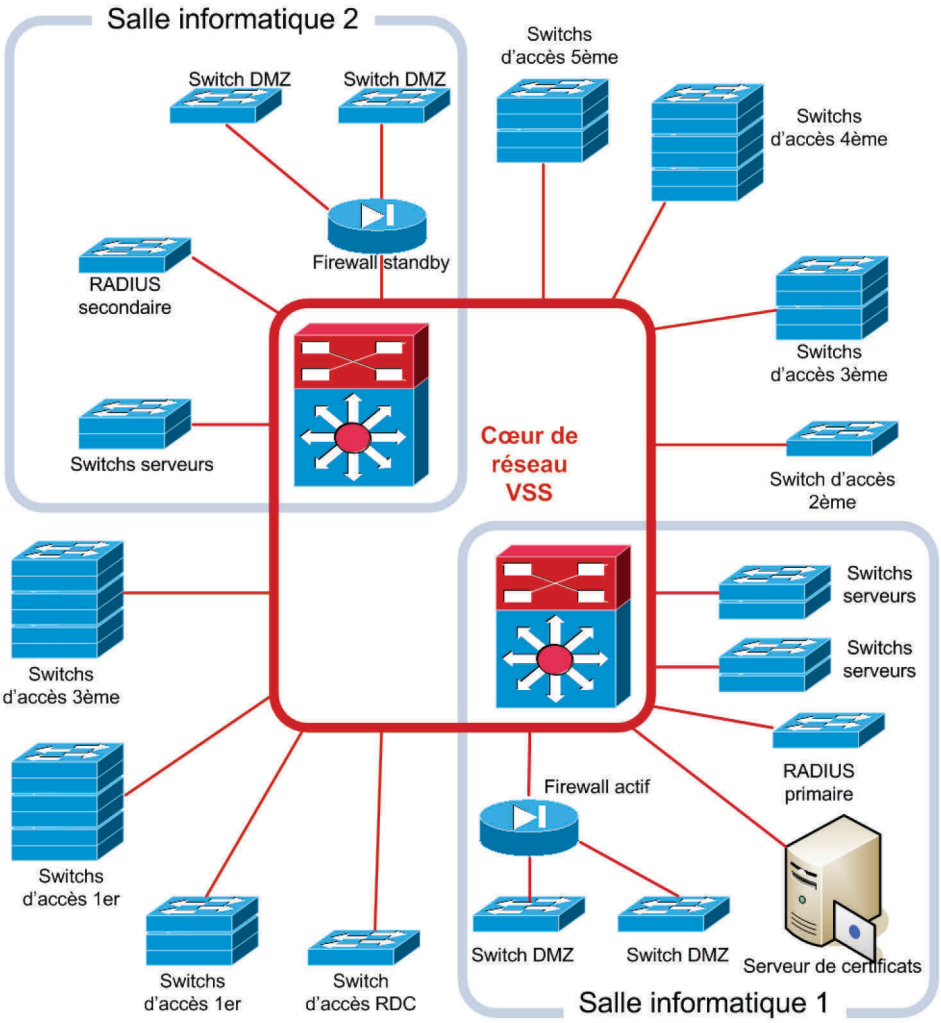


Figure 12: Architecture réseau du site Orléans Jaurès.

6. Le protocole 802.1x

Sphéria Val de France souhaite que la solution à sa problématique réponde à l'objectif suivant : vérifier l'identité des équipements voulant se connecter à son réseau afin de les autoriser ou non à se connecter.

Cette identification va être rendue possible par l'utilisation du protocole 802.1x qui effectue une authentification de l'équipement client au moment de la connexion physique au réseau.
La phase d'authentification sera assurée au travers du protocole EAP, le protocole 802.1x ne fournissant qu'un cadre fonctionnel à l'interaction entre les équipements. Il est donc nécessaire d'étudier les différentes méthodes d'authentification qu'il propose afin de choisir celles qui sont le plus adapté à l'environnement de SVF.

6.1. Principe général du protocole 802.1x

Le protocole 802.1x est composé de trois entités qui interagissent pour le processus d'authentification :

- Le système à authentifier ou Supplicant,
- Le système authentificateur ou Authenticator : c'est un équipement réseau (commutateur, routeur, borne wifi …) qui agit comme une barrière de sécurité entre le Supplicant et le réseau protégé. Il sert de relais entre le Supplicant et le serveur d'authentification et gère le PAE (Port Access Entity) qui permet au Supplicant d'accéder ou non au réseau,
- Le serveur d'authentification ou Authentication Server : il s'agit généralement d'un serveur RADIUS.

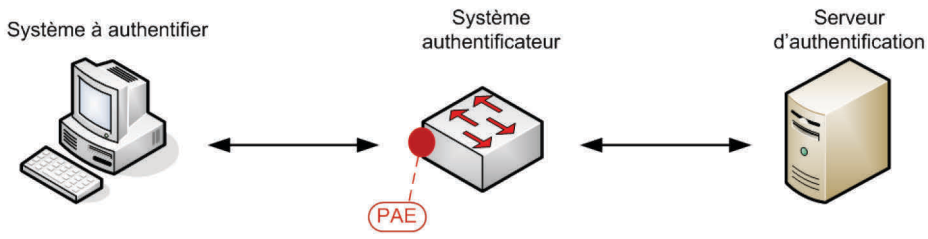


Figure 13: Les 3 entités qui interagissent dans le protocole 802.1x.

6.2. Le point d'accès au réseau : PAE

Le PAE est le point d'accès physique au réseau géré par le système authentificateur et sur lequel va être réalisée l'authentification. Dans le cas d'un commutateur il s'agit du port de connexion.

La principale innovation du protocole 802.1x réside dans ce concept : le port physique est scindé en deux ports logiques :

- Un port appelé « non contrôlé », qui gère toutes les trames spécifiques au protocole 802.1x et qui est toujours connecté,
- Un port appelé « contrôlé » qui peut être soit ouvert, soit fermé.

Ainsi avant l'authentification du demandeur, seul le mode non contrôlé est possible, permettant les échanges d'information d'authentification. Ces flux sont appelés flux EAPOL (EAP Over Lan).

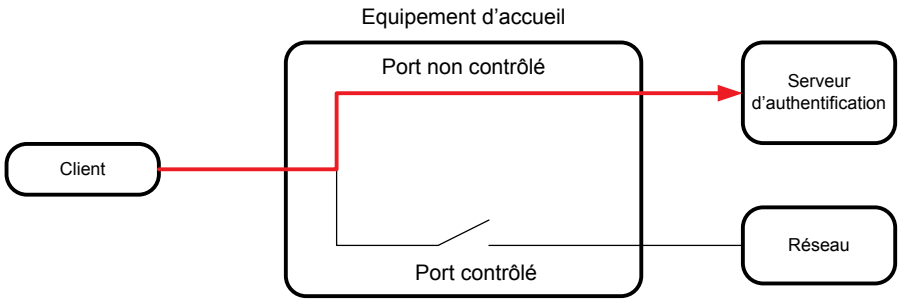


Figure 14: État du PAE avant la phase d'authentification.

Une fois que l'authentification est réalisée avec succès, le port contrôlé est basculé de l'état ouvert à l'état fermé et les flux autorisés peuvent être émis à destination du réseau.

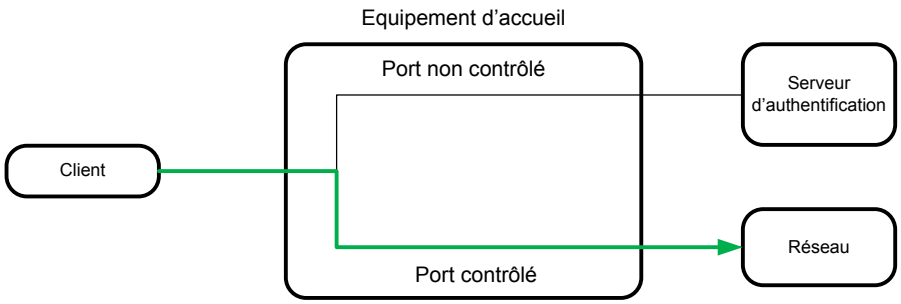


Figure 15: État du PAE après une authentification réussie.

6.3. Fonctionnement du protocole 802.1x

Comme je l'ai indiqué précédemment, le protocole 802.1x implique trois composants : le système à authentifier, l'authentificateur et le serveur d'authentification.

Il convient toutefois de noter que bien que les différentes conversations entre le client, l'authentificateur et le serveur d'authentification (et les protocoles utilisés) sont par un abus de langage communément appelées 802.1x, en réalité seule la conversation entre l'authentificateur et le client est 802.1x (ou EAPOL).

La communication entre le serveur d'authentification et l'authentificateur utilise le protocole RADIUS alors que la conversation entre le serveur d'authentification et le système à authentifier s'appuie sur le protocole EAP et les EAP-Methods.

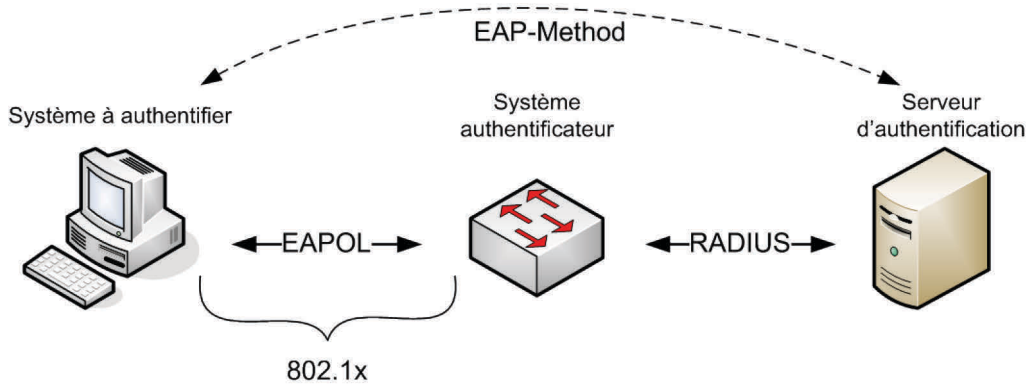


Figure 16: Les différents protocoles composant le 802.1x.

Le point clé du fonctionnement du protocole 802.1x est que le client ne peut communiquer qu'avec l'authentificateur.

Dans la phase d'authentification 802.1x, le système authentificateur se comporte comme un mandataire entre le système à authentifier et le serveur d'authentification.

Si l'authentification réussit, le système authentificateur donne l'accès à la ressource qu'il contrôle.

Le serveur d'authentification va quant à lui gérer l'authentification proprement dite en vérifiant les informations d'authentification du système à authentifier.

On peut considérer qu'il existe 4 scénarios d'interactions qui couvrent l'ensemble des cas que l'on peut rencontrer.

6.3.1. *Scénario 1 : Processus de base*

L'authentificateur va initier le processus d'authentification lorsqu'il détecte une connexion sur l'un de ses ports. S'il obtient une réponse à sa requête d'identité, il contacte le serveur RADIUS pour valider le contenu de la réponse. Le serveur RADIUS lui indique alors si le client est autorisé à se connecter au réseau.

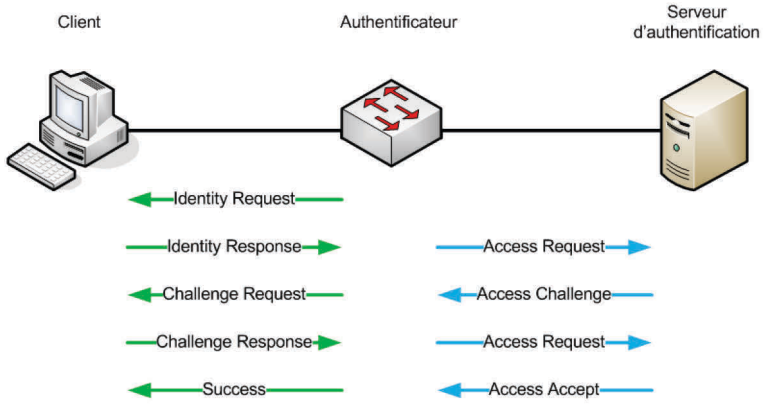


Figure 17: Exemple de dialogue lors du processus d'authentification.

6.3.2. *Scénario 2 : Supplicant non configuré*

Le Supplicant n'est pas configuré pour le 802.1x, l'Authentificateur ne reçoit pas de réponse à ses requêtes d'identité, il place alors le Supplicant dans un vlan Guest ou désactive le port sur lequel la connexion intervient.

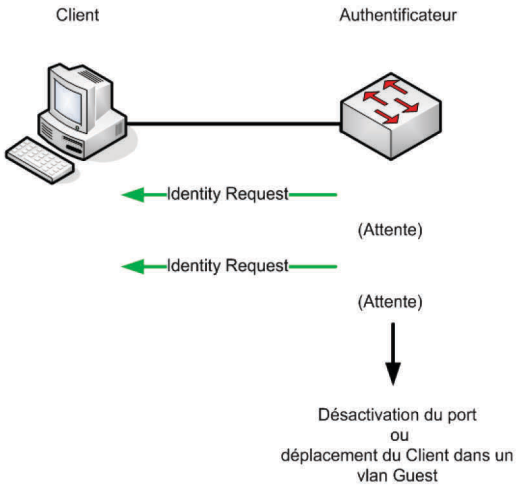


Figure 18: Exemple de dialogue lorsque le Supplicant n'est pas configuré.

6.3.3. *Scénario 3 : Pas d'authentificateur*

Le Supplicant est connecté sur un port sur lequel le 802.1x n'est pas activé.

Le Supplicant a 2 choix :

- Etre passif et attendre une requête d'identité EAPOL de la part de l'Authentificateur,

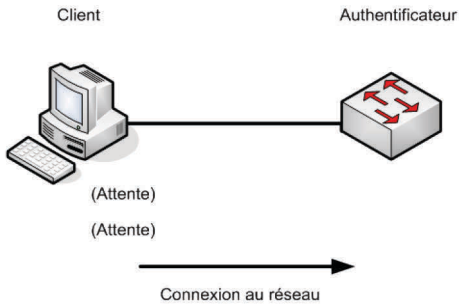


Figure 19: Exemple de dialogue sans authentificateur, Supplicant en mode passif.

- Emettre une requête EAPOL-Start qui va demander à l'Authentificateur de commencer le processus.

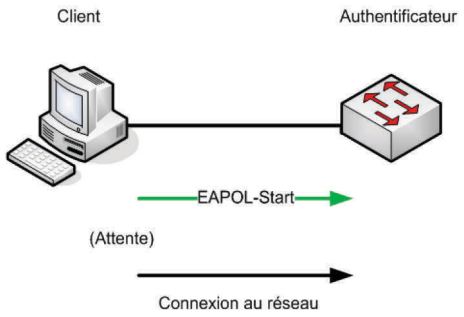


Figure 20: Exemple de dialogue sans authentificateur, Supplicant en mode actif.

Dans tous les cas le Supplicant ne recevra pas de réponse. Il arrêtera d'essayer de s'authentifier et se connectera au réseau.

6.3.4. *Scénario 4 : Pas de serveur d'authentification*

Dans ce dernier scénario le Supplicant et l'Authentificateur sont bien présents mais il manque le serveur d'authentification ou celui-ci est injoignable.

Lors des premières implémentations du protocole ce cas faisait que le port de l'Authentificateur était systématiquement laissé à l'état non-autorisé. Désormais le Supplicant peut être placé dans un vlan Guest ou autorisé à accéder au réseau selon la configuration de l'Authentificateur.

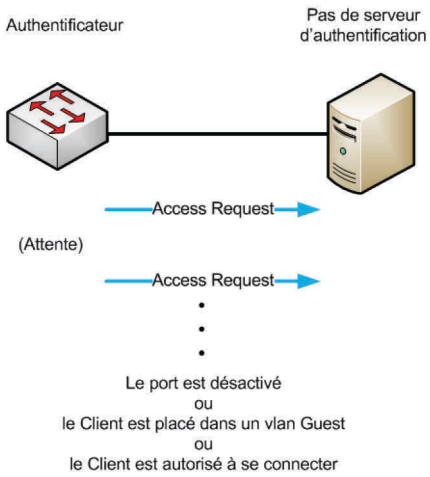


Figure 21: Exemple de dialogue sans serveur d'authentification.

7. Le protocole EAP

Le protocole 802.1x est une extension du protocole EAP aux environnements LAN. Ce protocole est utilisé pour transporter les informations d'authentification entre deux équipements.

Le protocole 802.1x ne propose pas qu'une seule méthode d'authentification, mais une trame sur laquelle sont basés plusieurs types d'authentification appelés méthodes.

Figure 22: Encapsulation des trames EAP.

7.1. Extensible Authentication Protocol (EAP)

Le protocole EAP est utilisé pour le transport et la gestion de l'authentification entre le Supplicant et le serveur d'authentification. Cela comprend la négociation sur la façon dont l'authentification va se mettre en place, quelle méthode sera utilisée, l'échange des informations d'identification définies dans la méthode et la déclaration finale de succès ou d'erreur.

Toutes les communications entre l'Authentificateur et le Supplicant sont très simples :

- L'Authentificateur demande de l'information,
- le Supplicant répond.

Le protocole EAP n'intègre pas de mécanisme de sécurité pour la transmission des informations.

Il existe quatre types de paquets utilisés par le protocole EAP :

Tableau II: Types de paquets EAP.

EAP Code	Valeur
Request	1
Response	2
Success	3
Failure	4

Une trame EAP est composée de 4 champs :

- Code : ce champ indique le type de paquet,
- Identifier : ce champ indique à quelle requête correspond une réponse,
- Length : ce champ indique la longueur du paquet EAP,
- EAP-Data : le contenu de ce champ varie selon le type de paquet EAP.

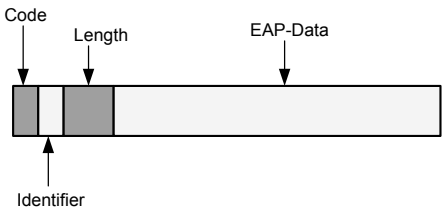


Figure 23: Format du paquet EAP.

Seuls les 2 premiers champs sont réellement pertinents pour EAP.
Le 1er, « Code », identifie quel type de paquets EAP est utilisé. Le second, « Identifier », permet de s'assurer que la séquence de trames est correcte.

C'est l'Authentificateur qui fixe la valeur du champ « Identifier », le Supplicant retourne la même valeur dans sa réponse. L'Authentificateur modifiera la valeur à la requête suivante et le Supplicant répondra avec cette nouvelle valeur.
Le diagramme ci-dessous illustre l'utilisation du champ « Identifier » dans une communication entre un Supplicant et un Authentificateur.

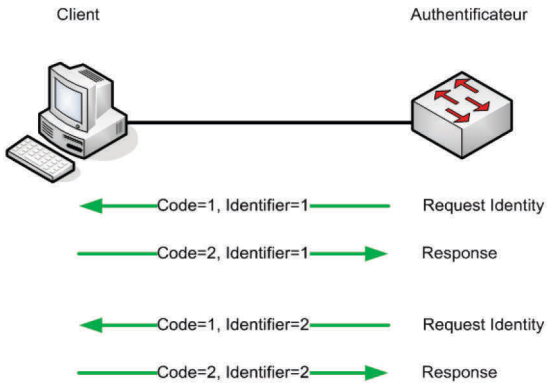


Figure 24: Exemple d'un dialogue EAP.

EAP est un protocole simple qui place trois couches au-dessus de la couche liaison IEEE 802 :

- la couche EAP : elle reçoit et envoie les paquets vers la couche basse (802) et transmet les paquets de type Request, Success et Failure à la couche EAP-Peer. Les paquets Response sont transmis à la couche EAP-Authenticator.
- les couches EAP-Peer et EAP-Authenticator : la couche EAP Peer est implémentée sur le Supplicant tandis que la couche EAP Authenticator est implémentée sur l'Authentificateur et le serveur d'authentification. Ces couches ont pour rôle d'interpréter le type de paquet Request ou Response et de les diriger vers la couche EAP-Method correspondant à la méthode d'authentification utilisée.
- la couche EAP-Method : elle traite la donnée encapsulée dans un paquet EAP qui correspond à l'information d'authentification échangée entre le Supplicant et le serveur d'authentification. La nature de la donnée d'authentification qui peut être transportée par un paquet particulier est dépendante du type EAP. Par exemple, un

paquet EAP de type Response ne peut transporter un challenge MD5. Il s'agit nécessairement dans ce cas d'un paquet de type Request-Identity.

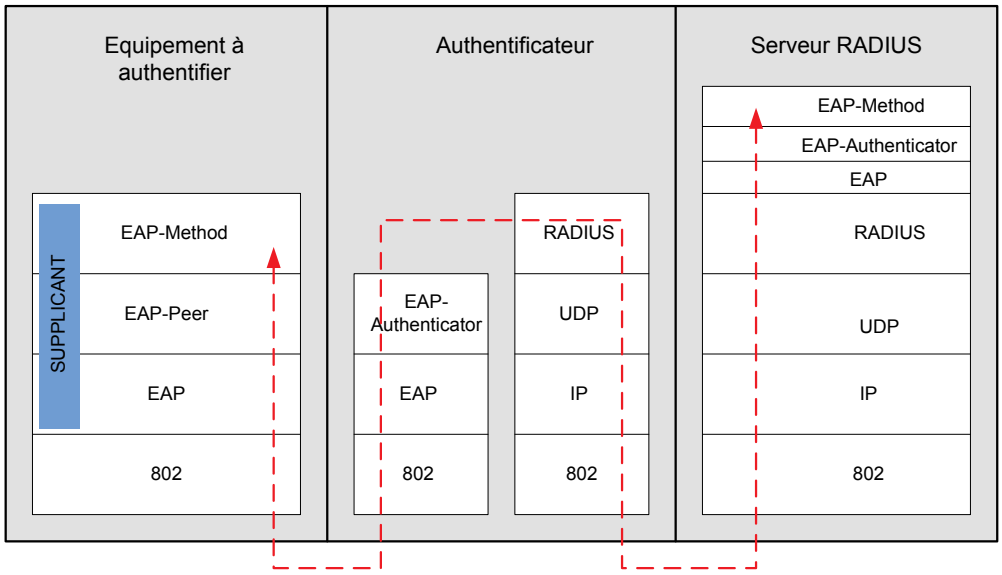


Figure 25: Les différentes couches du protocole EAP.

7.2. Extensible Authentication Protocol Over LAN (EAPOL)

EAP avait initialement été créé comme un protocole pour les liaisons point à point. EAPOL, lui, est défini dans le standard 802.1x pour adapter EAP au fonctionnement dans les environnements LAN.

Ce protocole travaille au niveau de la couche 2 (liaison) du modèle OSI et tire avantage du standard 802.1d qui est requis par tous les réseaux de type 802.

Cette intégration permet aux paquets 802.1x d'être les premiers envoyés sur le réseau lorsque le lien s'active entre le Supplicant et l'Authentificateur, avant les requêtes DHCP par exemple.

Le protocole 802.1x utilise pour ce faire, un groupe d'adresses définies mais non utilisées par le protocole Spanning-Tree qui est 01:80:C2:00:00:03.

Pour cela EAPOL ajoute trois champs aux paquets EAP :

- Version : ce champ indique la version du protocole EAPOL utilisé,
- Type : ce champ indique le type de paquet EAPOL,
- Longueur : ce champ indique la longueur du message qui suit.

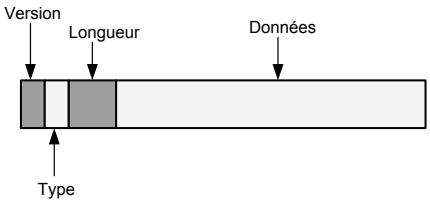


Figure 26: Format du paquet EAPOL.

Les différents types de paquets EAPOL sont :

- EAPOL-Start : le client annonce au système authentificateur qu'il souhaite se connecter,
- EAPOL-Key : échange des clés de cryptage,
- EAP-Packet : paquets qui encapsulent les paquets EAP,
- EAPOL-Logoff : le client demande la fermeture de la session,
- EAPOL-Encapsulated-ASF-Alert : ce paquet est utilisé lorsque le client doit envoyer une information avant que la phase d'authentification soit complétée.

7.3. Les méthodes EAP ou EAP-Methods

Une méthode EAP correspond à la façon dont une authentification est conduite. C'est une méthode particulière utilisée pour réaliser une authentification en utilisant EAP comme mécanisme de transport.

La trame EAP-Method est composée de 3 champs : EAP-Method Code, EAP-Method Data Length et EAP-Method Data.

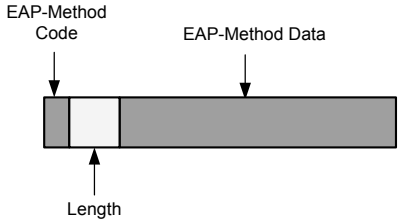


Figure 27: Format du paquet EAP-Method.

Comme précédemment le champ Data est simplement une encapsulation de l'information qui sera utilisée par le serveur d'authentification. Pour réaliser l'authentification, un accord doit être trouvé entre le Supplicant et le serveur d'authentification sur la méthode de chiffrement qui sera utilisée, c'est le rôle du champ Code.

Il existe un certain nombre de méthodes EAP, chacune disposant d'avantages et d'inconvénients notamment en termes de sécurité. Voici les méthodes les plus fréquemment utilisées.

7.3.1. EAP-MD5

Ce protocole initialement défini dans la RFC 2284 offre une sécurité minimale. Le client s'authentifie par un couple login/mot de passe. Le serveur envoie une valeur aléatoire, le client concatène cette valeur avec le mot de passe, calcule une empreinte à l'aide de l'algorithme MD5 qu'il renvoie au serveur. Le serveur calcule sa propre empreinte car il connait le mot de passe et compare les deux. En fonction du résultat, il valide ou non l'authentification.

- Avantage
  - Le seul avantage est la simplicité. Cette méthode est très facile à mettre en place.

- Inconvénients
  - Cette méthode est vulnérable aux attaques par dictionnaire hors-ligne,

- Les échanges ne sont pas chiffrés et cette méthode ne gère pas la distribution dynamique des clés WEP.

7.3.2. EAP-TLS (Tunneled Transport Layer Security)

EAP-TLS est un protocole basé sur l'utilisation de certificats, il dispose de trois fonctions :

- L'authentification du serveur,
- L'authentification du client,
- Le chiffrement.

L'utilisation de certificats accroît le nombre d'échanges nécessaires entre le Supplicant et le serveur d'authentification. Ceci a néanmoins un impact très faible sur le réseau concerné mais peut accroître le temps nécessaire pour l'authentification et avoir un impact sur les applications sensibles.

- Avantages
  - Le système de certificat est plus sûr que les mots de passe, une authentification mutuelle est réalisée entre le serveur et le client en échangeant les certificats suivant le protocole TLS.
  - Il est proposé nativement dans Windows XP.

- Inconvénients
  - Il est nécessaire de disposer d'une infrastructure pour la gestion des certificats (PKI),
  - La charge induite par les opérations de gestion de certificats est à prendre en compte. La distribution des certificats aux clients n'est pas non plus à négliger,
  - Il est possible d'exporter la clé privée du client. Dans ce cas, il est nécessaire de révoquer le certificat.

7.3.3. EAP-MS-CHAPV2

Ce protocole a été développé par Microsoft, il est basé sur un mécanisme d'authentification mutuelle.

Il a été créé à l'origine comme un protocole d'authentification pour les connexions point à point. Il est toutefois vulnérable aux attaques par dictionnaire hors-ligne.

- Avantages
    - Proposé nativement dans Windows XP,

- Inconvénient
    - Ce protocole ne sécurise pas l'accès au réseau s'il est utilisé seul.

7.3.4. EAP-PEAP (Protected EAP)

Ce protocole est plus communément appelé PEAP et comme son nom l'indique (Protected EAP), il protège les échanges EAP.

Il a été développé conjointement par Microsoft, Cisco et RSA Security pour pallier le principal défaut d'EAP/TLS, à savoir la nécessité de distribuer des certificats à tous les utilisateurs ou clients.

Comme avec EAP/TLS une authentification mutuelle s'établit entre le Supplicant et le serveur. Cependant ici elle est asymétrique : le serveur sera authentifié par son certificat auprès du Supplicant tandis que ce dernier s'authentifiera auprès du serveur à l'aide d'un identifiant et d'un mot de passe.

Le processus d'authentification se déroule en 2 phases :

- la 1ère phase sert à établir un tunnel TLS entre le Supplicant et le serveur d'authentification,
- la seconde phase sert à l'authentification du couple identifiant-mot de passe.

Seul le serveur a besoin d'un certificat, mais les clients doivent tout de même installer le certificat de l'autorité qui a émis le certificat du serveur.

Une des méthodes les plus populaires pour la seconde phase est EAP-MS-CHAPV2. Comme les identifiants sont échangés à l'intérieur d'un tunnel, il n'y a pas de risque d'espionnage, ceci élimine ainsi l'un des vulnérabilités de MS-CHAPV2.

- Avantages
    - Le client peut être authentifié par mot de passe : c'est une simplification de gestion par rapport à EAP-TLS, tout en proposant une authentification mutuelle sécurisée.
    - PEAP est proposé nativement dans Windows XP.

- Inconvénients
    - L'utilisation d'une méthode d'authentification par mot de passe rend vulnérable aux attaques par dictionnaire en ligne,
    - Il convient de configurer le serveur pour qu'il détecte et bloque les attaques de type dictionnaire,
    - Cisco et Microsoft ont distribué des versions différentes de PEAP, il faut donc s'assurer que la méthode d'authentification est compatible.

7.3.5. EAP-TTLS (Tunneled TLS)

EAP-TTLS est une méthode propriétaire, conçue par la société Funk Software en tant qu'extension d'EAP-TLS.
Elle est similaire à la méthode PEAP car toutes les deux commencent par établir un tunnel TLS puis mettent en œuvre une autre méthode d'authentification.

La différence principale entre ces deux méthodes vient de la manière dont sont encapsulés les échanges dans la deuxième phase. TTLS utilise des AVP (Attribute Values Pairs) encapsulés dans des paquets EAP-TTLS et compatibles avec ceux de RADIUS ce qui simplifie les échanges entre le serveur EAP-TTLS et le serveur RADIUS qui contient les informations relatives aux utilisateurs, dans le cas où celles-ci ne sont pas directement stockées sur le serveur EAP-TTLS.

- Avantages
    - Comme PEAP, TTLS autorise tout type d'authentification interne à l'intérieur du tunnel TLS,
    - Utilisation des AVP pour envoyer des paramètres de connexion au client,
    - Les AVP sont compatibles avec les AVP RADIUS.

- Inconvénients
    - EAP-TTLS n'est pas intégré nativement au système d'exploitation Windows XP,
    - Méthode d'authentification propriétaire,
    - Méthode d'authentification par mot de passe vulnérable aux attaques par dictionnaires (mais pas hors-ligne),
    - Il convient de configurer le serveur pour qu'il détecte et bloque les attaques par dictionnaires.

7.3.6. LEAP (Lightweight Extensible Authentication Protocol)

Ce protocole a été développé par Cisco pour les réseaux sans fil. Il fournit des clés WEP dynamiques par session et par utilisateur à chaque fois qu'un utilisateur s'authentifie et repose sur une authentification mutuelle via un couple identifiant/mot de passe.
Ce protocole est dérivé de MS-CHAP de Microsoft.

- Avantages

  Solution simple à mettre en œuvre avec des équipements Cisco ou compatible.

- Inconvénients
    - LEAP n'est pas intégré nativement à Windows XP,
    - Méthode d'authentification propriétaire (Cisco),
    - Vulnérable aux attaques par dictionnaire comme EAP-MD5.

7.3.7. EAP-FAST (Flexible Authentication via Secure Tunneling)

Il s'agit ici également d'une méthode propriétaire Cisco publiée en avril 2005 sous forme de *draft* IETF. Ce protocole est très proche de EAP-TTLS, mais la différence se situe au niveau

du tunnel créé pour protéger l'authentification : il est établi avec un algorithme de cryptage symétrique qui s'appuie sur des fichiers protégés par mot de passe, appelés PAC (Protected Access Credential).
Le principal avantage de ce protocole est donc qu'il ne requiert pas l'utilisation de certificats, mais à l'usage la gestion des PAC est relativement contraignante car ils sont propres à chaque utilisateur.

- Avantages
    - Pas d'installation de serveur de certificat,
    - Réauthentification rapide (fast) : très important pour les utilisateurs nomades.

- Inconvénients
    - EAP-FAST n'est pas intégré nativement à Windows XP,
    - C'est une méthode d'authentification propriétaire (Cisco),
    - Le protocole d'authentification lourd en gestion (PAC).

7.4. Les failles du protocole EAP

Il existe trois principales failles pour le protocole EAP :

- Attaquer la méthode EAP sur ses propres failles,
- Attaquer une session déjà établie,
- S'intercaler entre le système authentificateur et le client afin d'être authentifié à la place de ce dernier (attaque de type Man In the Middle).

7.4.1. Attaque par dictionnaire hors-ligne

Lors de l'utilisation de la méthode EAP-MD5, par exemple, le serveur envoie un défi au client. Celui-ci le concatène avec son mot de passe, crypte ce dernier avec le protocole MD5 pour obtenir un hash et le transmet au serveur. Le serveur qui connait le mot de passe, effectue la même opération et compare les résultats.
En procédant à une écoute du réseau, le pirate peut identifier le hash du défi et le défi lui-même qui transitent. Ensuite, le pirate va concaténer un mot de passe au hasard avec le défi puis le crypter via MD5. Il pourra alors comparer le hash obtenu avec celui espionné plus tôt.

Avec une multitude de combinaisons il finira par trouver le mot de passe qui donnera le bon hash.
Cette attaque est dite « hors-ligne » car le pirate peut retrouver le mot de passe sans avoir à le soumettre au serveur.

La solution est d'utiliser, si cela est possible, une méthode d'authentification infaillible aux attaques par dictionnaire hors-ligne.

7.4.2. Attaque par dictionnaire en ligne

Si l'on utilise toujours une authentification MD5 mais cette fois dans un tunnel sécurisé avec PEAP, TTLS ou EAP-Fast, le pirate peut tout de même réaliser une attaque. Seulement, cette fois ci elle sera dite « en ligne » car il sera obligé de solliciter le serveur d'authentification à chaque tentative de connexion.

La solution dans ce cas est d'interdire sur le serveur d'authentification plus de trois tentatives de connexion. Il peut d'ailleurs être intéressant d'avertir les administrateurs du réseau, via des remontées d'alertes ou les journaux d'évènements, qu'un système a tenté de se connecter plusieurs fois sans succès.

7.4.3. Attaque de la session

Le protocole EAP à lui seul ne protège pas la session. En effet, une fois la connexion établie le client diffuse ses paquets en clair et le système authentificateur se contente de vérifier que l'adresse MAC a déjà été autorisée. Un pirate peut donc attendre que le client s'authentifie pour ensuite usurper son adresse MAC (ARP spoofing) et ainsi se faire passer pour le client sur le réseau.
Ceci est d'ailleurs valable pour la méthode EAP-TLS car celle-ci permet de sécuriser la phase d'authentification mais ne prévoit rien sur la protection de la session.

La solution reste de mettre en place un tunnel entre le système à authentifier et le système authentificateur tout au long de la connexion. Il faut bien entendu que ce tunnel utilise un cryptage relativement puissant.

7.4.4. Attaques MIM (Man in the Middle)

Dans ce type d'attaque, le pirate doit s'insérer pendant le processus d'authentification entre le client et le serveur. Son ordinateur se comporte alors comme un système authentification vis-à-vis du client et utilise les informations fournies par le client pour se faire authentifier à sa place par le serveur.
Les authentifications sécurisées par un tunnel ne sont pas à l'abri de ce type d'attaque. Le pirate peut via un faux certificat se faire passer pour le serveur d'authentification afin d'ouvrir le tunnel avec le client et utiliser le certificat du client pour ouvrir un tunnel avec le serveur.

La solution est d'enregistrer le certificat du serveur dans les clients pour qu'il puisse le comparer avec celui transmis par le serveur à chaque phase d'authentification.

8. Le protocole RADIUS

Le protocole RADIUS a été normalisé par l'IETF en 2000 dans deux RFC :

- RFC 2865 : elle est la référence principale du protocole RADIUS,
- RFC 2866 : elle définie les fonctionnalités de comptabilisation pour permettre la journalisation et la facturation des accès.

A l'origine ce protocole a été créé pour permettre aux fournisseurs d'accès à internet d'authentifier les utilisateurs distants à partir d'une seule base utilisateurs malgré une multitude de serveurs.
Le protocole RADIUS permet de faire la liaison entre les besoins d'identification et une base d'utilisateurs en assurant le transport des données d'authentification de façon normalisée.
Le serveur traite la requête cliente en accédant si nécessaire à une base externe : base de données SQL, annuaire LDAP, comptes d'utilisateur de machine ou de domaine.

RADIUS est un protocole qui répond au modèle AAA dont les initiales résument les trois fonctions du protocole :

- Authentication : authentifier l'identité du client,
- Authorization : accorder des droits au client,
- Accounting : enregistrer les données de comptabilité de l'utilisation du réseau.

La première tâche de ce serveur est donc d'authentifier les requêtes qui lui parviennent d'un poste client.
On peut distinguer deux types de « preuves » d'identité d'un client : un mot de passe ou un certificat électronique.

L'authentification peut être suffisante en elle-même dans un réseau à plat où tous les postes de travail sont considérés de façon équivalente. Cependant lorsqu'un réseau est segmenté, se pose la question de ce que l'on fait du poste authentifié : où doit il être placé dans le réseau ? Dans quel vlan doit il être mis ?
C'est là la deuxième tâche du serveur, il va délivrer les autorisations en indiquant par exemple le numéro du vlan dans lequel le client doit être placé.

L'implémentation du serveur RADIUS tient compte du fait que tous les équipements ne sont pas nécessairement compatibles 802.1x, ceci est alors réalisé par l'authentification RADIUS-MAC.

8.1. Principe de l'authentification RADIUS-MAC

L'authentification par adresse MAC, appelée RADIUS-MAC, est la plus simple à mettre en œuvre mais est également la moins sûre.

Les étapes du protocole sont les suivantes:

- Le poste de travail se branche sur un des ports du commutateur (1),
- Le commutateur détecte cette connexion et envoie une requête d'authentification au serveur RADIUS (2). Dans cette requête, l'adresse MAC du poste fait office d'identifiant,
- Le serveur reçoit la demande et vérifie si l'adresse MAC est présente dans sa base (3). Il peut également récupérer le vlan auquel sera connecté le poste, si cette information est connue,
- Le serveur envoie la réponse au commutateur (4) :
    - Si la réponse est positive, le commutateur ouvre le port sur le vlan indiqué,
    - Si la réponse est négative, le port du commutateur reste fermé.

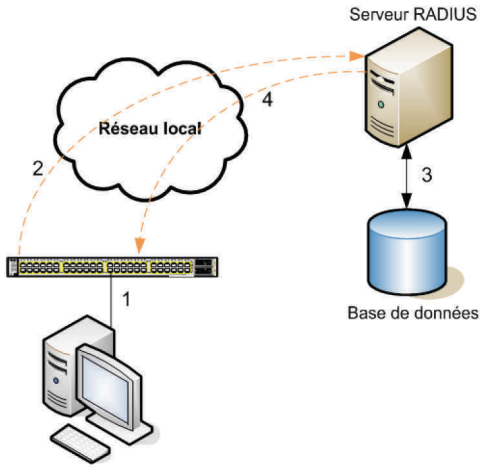


Figure 28: Principe de l'authentification RADIUS-MAC.

Dans ce type d'authentification il n'y a pas de communication entre le poste de travail et le serveur RADIUS. Tous les échanges interviennent entre le commutateur et le serveur.

8.2. Principe de l'authentification 802.1x

La différence la plus importante avec l'authentification par adresse MAC est que dans le cas de l'authentification 802.1x, un composant logiciel sur le client est indispensable. Il s'agit du supplicant et c'est lui qui va envoyer les éléments d'authentification (certificat, identifiant, mot de passe …) au serveur RADIUS.

Les étapes du protocole sont les suivantes:

- Le poste de travail envoie au commutateur ses informations d'authentification (1),
- Le commutateur sert d'intermédiaire et relais la requête d'authentification au serveur RADIUS (2).
- Le serveur reçoit la demande et vérifie si l'identifiant (et non plus l'adresse MAC) est présent dans sa base (3). Il peut également récupérer le vlan auquel sera connecté le poste, si cette information est connue,
- Le serveur envoie la réponse au commutateur (4) :
    - Si la réponse est positive, le commutateur ouvre le port sur le vlan indiqué,
    - Si la réponse est négative, le port du commutateur reste fermé.

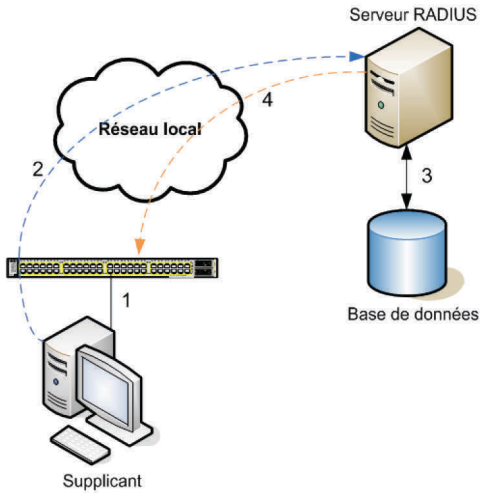


Figure 29: Principe de l'authentification 802.1x.

Dans ce type d'authentification, le commutateur sert d'intermédiaire durant la totalité des échanges entre le Supplicant et le serveur RADIUS

8.3. Description du protocole RADIUS

Le protocole établit une couche applicative au-dessus de la couche de transport UDP, les ports utilisés sont :

- 1812 : pour recevoir les requêtes d'authentification et d'autorisation,
- 1813 : pour recevoir les requêtes de comptabilité.

RADIUS utilise quatre types de paquets pour assurer les transactions d'authentification.

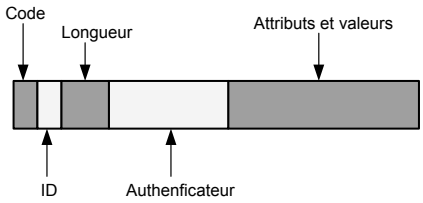


Figure 30: Format du paquet RADIUS.

- Code : Ce champ identifie le type de paquet
  - Access-Request : 1,
  - Access-Accept : 2,
  - Acces-Reject : 3,
  - Access-Challenge : 11,
- ID : Ce champ permet au client RADIUS d'associer les requêtes et les réponses,
- Longueur : Ce champ contient la longueur totale du paquet,
- Authentificateur : Ce champ a pour but de vérifier l'intégrité du paquet. Il permet de vérifier que la requête n'a pas été modifiée pendant la transmission,
- Attributs et valeurs : Ce champ contient les attributs qui sont envoyés soit par le commutateur soit par le serveur.

8.3.1. Les types de paquets RADIUS

- Paquet Access-Request

La communication avec le serveur RADIUS commence toujours par ce paquet. Il contient généralement l'attribut User-Name ainsi que l'identifiant du système authentificateur émetteur.

- Paquet Access-Accept

Ce paquet est renvoyé au commutateur par le serveur RADIUS si l'authentification contenue dans le paquet Access-Request a été validée. Ce paquet spécifie au commutateur les autorisations accordées par le serveur.

- Paquet Access-Reject

Ce paquet est envoyé par le serveur RADIUS si l'authentification a échouée.

- Paquet Access-Challenge

Ce paquet est toujours utilisé avec le protocole EAP car il permet au serveur de demander un certificat ou un mot de passe au système à authentifier.

8.3.2. Les attributs RADIUS

Les attributs sont le principe le plus important du protocole RADIUS car c'est eux qui véhiculent les informations nécessaires aux systèmes authentificateurs pour assurer les connexions.
La valeur d'un attribut peut correspondre à l'un des types suivants :

- Adresse IP,
- Date,
- Chaîne de caractères,
- Entier,
- Valeur binaire,
- Valeur parmi une liste de valeur.

Ces attributs et leur valeur sont appelés Attributes Value-Pair (AVP).

Le champ Attributs et Valeurs d'un paquet peut contenir plusieurs AVP comme le décrit le schéma ci-dessous :

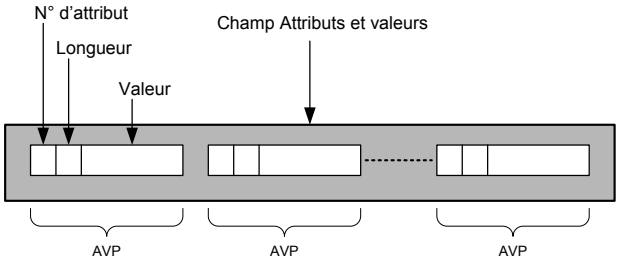


Figure 31: Format du champ Attributs et Valeurs.

Plus d'une centaine d'attributs sont par ailleurs définis soit dans la RFC 2865 soit dans les documentations des constructeurs puisqu'un attribut leur est réservé permettant d'encapsuler des attributs spécifiques au matériel.
On trouve par exemple les attributs suivants :

- User-Name,
- User-Password,
- CHAP-Password,
- Vendor-Specific,
- …

8.4.Synthèse

Comme nous venons de le voir, le protocole 802.1x est à même de répondre à la problématique de Sphéria Val de France car il permet d'authentifier les équipements se connectant au réseau. Cependant il faut désormais étudier la manière de l'intégrer dans l'environnement de SVF.

9. Le protocole 802.1x dans le contexte de SVF

Pour pouvoir mettre en œuvre l'architecture 802.1x il est nécessaire de bien identifier :

- Les différents équipements qui vont la composer,
- Les méthodes d'authentification supportées par ces équipements,
- Les impacts sur les processus organisationnels existants.

9.1. Les composants de l'architecture 802.1x chez SVF

Tout d'abord, je rappelle que le processus d'authentification consiste en l'interaction de 3 composants :

- Le système à authentifier,
- Le système authentificateur,
- Le serveur d'authentification.

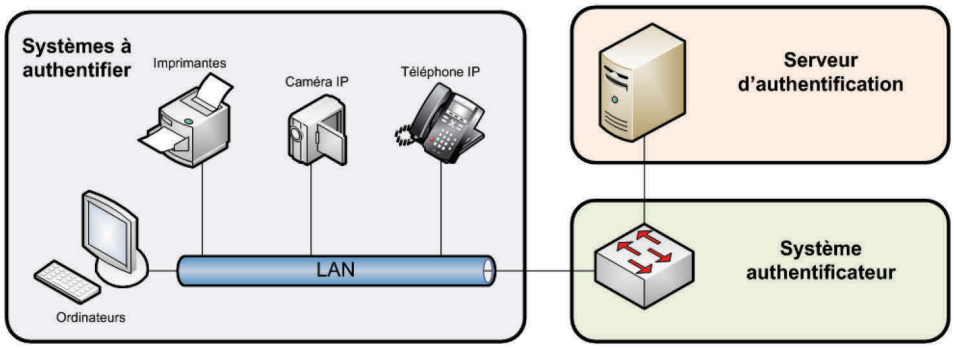


Figure 32: Les composants de l'architecture 802.1x chez SVF.

9.1.1. Les systèmes SVF à authentifier

Le réseau de SVF étant un réseau multiservices, plusieurs familles d'équipements doivent être authentifiées. Le tableau ci-dessous récapitule ces différents systèmes en indiquant s'ils sont à même de gérer le protocole 802.1x.

Tableau III: Liste des systèmes SVF à authentifier.

Système	Gestion du 802.1x
PC Windows XP	Oui
Imprimante réseau	Selon les modèles
Caméra IP	Oui
Téléphone IP	Oui
Visioconférence	Non
Badgeuse	Non
Équipement de GTB	Non

L'analyse des différents systèmes à authentifier est très importante pour déterminer les méthodes qui seront utilisées.

9.1.2. Les systèmes authentificateurs SVF

Les systèmes authentificateurs servent de relais dans le processus d'authentification. Dans le cas de SVF ce sont les commutateurs d'accès Cisco 3750E présents dans les locaux techniques des étages qui vont jouer ce rôle.

9.1.3. Le serveur d'authentification SVF

Le serveur RADIUS possède une fonction unique : s'assurer de l'identité des utilisateurs et des équipements entrant sur le réseau d'entreprise.
SVF dispose de deux serveurs d'authentification Cisco Secure ACS acquis en prévision de ce projet. Le choix de ces équipements s'est fait afin de garder une cohérence et limiter les problématiques de compatibilité par rapport aux autres équipements réseaux.

9.2. Les différents types de clients

L'étude préalable m'a permis de distinguer deux populations d'utilisateurs pour lesquels le Département Informatique sera amené à gérer le mode d'accès au réseau.

- Le personnel SVF

Le personnel du site Jean Jaurès de Sphéria Val de France est la première famille de client, avec leurs ordinateurs (fixes ou portables) cascadés sur les téléphones IP (ce mode de connexion a un impact sur la configuration des commutateurs).
Ces utilisateurs disposent d'un matériel qui est maitrisé par le DI.

- Les prestataires

Selon les besoins des différents prestataires trois cas de figure sont apparus avec des besoins différents.

- Cas de figure n°1 : Prestataire internet

Dans ce cas, le besoin du prestataire est uniquement un accès à internet. Le prestataire dispose de son ordinateur personnel sur lequel le DI SVF n'a aucune maitrise.
Il est donc nécessaire d'isoler ce matériel dans un vlan spécifique avec seulement l'accès à internet. De plus le mode d'authentification doit être simple.

- Cas de figure n°2 : Prestataire SI et internet

Dans ce cas, le prestataire doit pouvoir accéder au SI SVF et à internet.

- Cas de figure n°3 : Prestataire avec ses outils spécifiques

Dans ce cas, le prestataire doit pouvoir accéder au SI SVF ainsi qu'à internet et pouvoir utiliser des outils spécifiques que le DI SVF ne peut mettre à sa disposition.

- Avantages-inconvénients

Dans un premier temps évaluons les avantages et les inconvénients que ce soit pour le prestataire ou pour SVF si l'on autorise le prestataire à utiliser son ordinateur personnel.

Tableau IV: Comparatif des contraintes pour un ordinateur prestataire.

Avantages et inconvénients de l'utilisation d'un ordinateur portable personnel d'un prestataire			
Prestataire		**SVF**	
Avantages	Inconvénients	Avantages	Inconvénients
• Travaille dans son environnement	• Signature de la charte de fonctionnement du SI	• Aucun prêt d'ordinateur portable ou fixe	• Baisse du niveau de sécurité
• Rapidement prêt pour assurer sa prestation	• Configuration de leur ordinateur pour authentification 802.1x		• Mise en place de mesures de sécurité supplémentaire
• Aucune réinstallation des outils nécessaire à la prestation			• Configuration des PC des prestataires
			• Création procédure de configuration des PC prestataires
			• Création processus de gestion des habilitations des prestataires
			• Création de compte de connexion (proxy)
			• Risque de virus

Dans un second temps voyons les avantages et les inconvénients que ce soit pour le prestataire ou pour SVF si celle-ci met un ordinateur à disposition du prestataire.

Tableau V: Comparatif des contraintes pour un ordinateur de prêt SVF.

Avantages et inconvénients de l'utilisation d'un ordinateur de prêt SVF pour un prestataire?			
Prestataire		**SVF**	
Avantages	Inconvénients	Avantages	Inconvénients
• Aucune configuration 802.1x	• Ne travaille pas dans son environnement	• Augmentation du niveau sécurité	• Prêt d'ordinateur portable ou fixe
	• Réinstallation des outils nécessaire à la prestation	• Aucun risque de virus dû à la connexion de PC prestataire	• Risque d'allongement du temps de prestation
	• Signature de la charte de fonctionnement du SI	• Aucune configuration des PC des prestataires	• Création processus de gestion des habilitations des prestataires
	• Risque d'allongement du temps de prestation		• Création de compte de connexion (proxy)

Conclusion :

Comme on le voit, chaque solution dispose d'avantages et d'inconvénients pour les deux parties et peut avoir un impact non négligeable sur le fonctionnement du Département Informatique.

La décision prise par l'équipe projet, est que pour des raisons de souplesse[4] :

- Les prestataires utilisant des outils spécifiques pourront utiliser leur ordinateur personnel,
- Tous les autres se verront mettre à disposition un ordinateur SVF.

[4] Annexe 3.

9.3. Périmètre géographique de déploiement du 802.1x

Le choix dans le cadre de ce projet a été de se limiter à une implémentation du protocole 802.1x sur le bâtiment d'Orléans Jean Jaurès. Seules les prises alimentées par les commutateurs d'accès seront donc contrôlées : à savoir les bureaux, les salles de visioconférences, les prises disposées dans les couloirs et les faux plafonds.

L'accès aux salles informatiques étant strictement contrôlé par badge il n'est pas nécessaire de les inclure dans le périmètre.

10. Etude des méthodes d'authentification possibles

Les équipements compatibles 802.1x, désirant se connecter au réseau, peuvent gérer un ou plusieurs types d'authentification. Il est donc nécessaire d'étudier ces possibilités afin d'identifier le niveau de sécurité que l'on peut obtenir et de proposer une politique d'authentification adaptée à chaque cas.

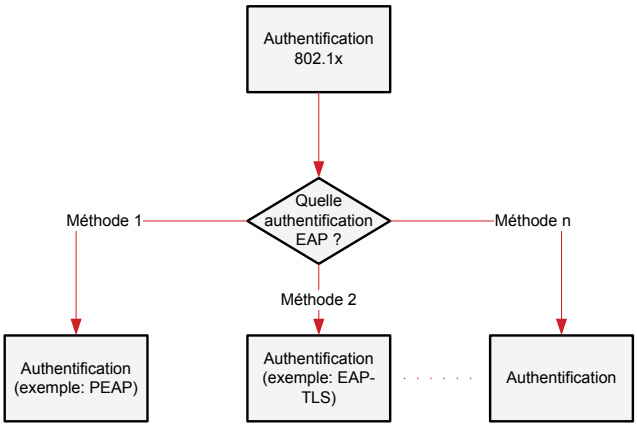


Figure 33: Méthodes d'authentification EAP.

10.1. Les systèmes EAP de SVF à authentifier

Comme je l'ai indiqué précédemment, le protocole 802.1x s'appuie sur le protocole EAP : il est indispensable d'identifier les méthodes d'authentification supportées par les différents systèmes à authentifier.

Voici les méthodes supportées par les différents systèmes présents chez SVF :

Tableau VI: Méthodes EAP supportées par système.

TYPE	Méthodes EAP gérées
PC sous Windows XP	MD5, LEAP, TLS, PEAP, FAST
Imprimante compatible 802.1x	MD5, TLS, PEAP
Téléphone IP	MD5, TLS
Caméra IP	TLS

10.2. Les systèmes EAP authentificateurs de SVF

Le système authentificateur ne sert que d'intermédiaire entre le client à authentifier et le serveur d'authentification, il ne fait que relayer les échanges et appliquer le résultat final que lui indiquera le serveur d'authentification.
La méthode d'authentification EAP utilisée n'a donc aucune importance dans son cas.

10.3. Le serveur d'authentification SVF

Le serveur d'authentification dont dispose SVF est un serveur RADIUS Cisco Secure ACS.
Voici la liste des méthodes d'authentification EAP qu'il supporte :

Tableau VII: Méthodes EAP supportées par Cisco ACS.

TYPE	Méthodes EAP gérées
RADIUS CISCO Secure ACS	MD5, LEAP, TLS, PEAP, FAST

L'intérêt d'EAP-FAST est qu'il peut vérifier plusieurs paramètres d'un système à authentifier comme :

- la version du système d'exploitation,
- la présence d'un antivirus et sa version sur le poste, …

Cependant, cette méthode n'est pas native au système d'exploitation utilisé chez Sphéria Val de France, en l'occurrence Windows XP Professionnel.

10.4. Le serveur d'annuaire SVF

Le serveur d'annuaire utilisé est Microsoft Active Directory.
Voici la liste des méthodes d'authentification EAP qu'il supporte :

Tableau VIII: Méthodes EAP supportées par Microsoft Active Directory.

TYPE	Méthodes EAP gérées
Microsoft Active Directory	LEAP, TLS, PEAP, FAST

10.5. Récapitulatif des méthodes EAP par système

Voici un tableau récapitulatif des méthodes d'authentification EAP gérées pour les systèmes à authentifier, le serveur d'authentification et le serveur d'annuaire.

Tableau IX: Récapitulatif des méthodes supportées par système.

Système	MD5	LEAP	TLS	TTLS	PEAP	FAST
Windows XP	**X**		**X**		**X**	
RADIUS Cisco	**X**	**X**	**X**		**X**	**X**
Active Directory		**X**	**X**	**X**	**X**	**X**
Imprimante	**X**		**X**		**X**	
Téléphone IP	**X**		**X**			
Caméra IP			**X**			

Ce tableau montre que le serveur RADIUS Cisco ne gère pas l'EAP-TTLS et que le serveur d'annuaire Active Directory ne gère pas l'EAP-MD5. C'est pourquoi je ne retiendrais pas ces méthodes d'authentification. On peut également exclure EAP-FAST qui dans le contexte SVF ne concernerait que le serveur RADIUS et le serveur d'annuaire.

11. Choix des méthodes d'authentification

L'objectif de cette étape est de répondre aux questions suivantes :

- Quelle méthode d'authentification utiliser pour les équipements ne gérant pas le 802.1x ?
- Quelle méthode d'authentification EAP utiliser pour les équipements gérant le 802.1x ?
- Comment protéger le réseau ?

11.1. Les méthodes d'authentification pour les équipements non 802.1x

Pour les équipements ne gérant pas le 802.1x, mon choix se porte sur une méthode simple qui est le filtrage par adresse MAC.
Le principe de cette méthode est de référencer dans le serveur d'authentification les adresses MAC dites valides. Lors de la connexion au réseau, le client envoie son adresse MAC au serveur qui vérifie sa présence dans sa base de données.

Il est par contre nécessaire de limiter les requêtes de connexion provenant du même émetteur pour éviter les attaques.

Un point important concerne les caméras IP : bien qu'étant compatibles 802.1x, elles seront authentifiées par leur adresse MAC. Ce choix s'impose par le fait que ces équipements ne sont pas sous la responsabilité du Département Informatique et donc que celui-ci ne peut intervenir sur le paramétrage et l'administration nécessaire à un fonctionnement 802.1x.
Un autre point concerne les imprimantes qui ne sont pas toutes compatibles avec le 802.1x. Ainsi pour garder une uniformité de gestion, je considère plus judicieux de les authentifier par leur adresse MAC.

Les équipements concernés par le filtrage par adresse MAC sont donc :

- Les imprimantes,
- Les badgeuses,
- Les équipements de GTB,
- Les terminaux de visioconférence,
- Les caméras IP.

La procédure de migration qui sera mise en place devra tenir compte des équipements actuellement connectés au réseau sur des ports non 802.1x afin d'assurer une continuité de service.

11.2. Les méthodes d'authentification pour les équipements 802.1x

L'analyse des besoins m'a amené au choix de deux types d'authentification :

- Une authentification de la machine pour les téléphones IP et les ordinateurs SVF,
- Une authentification de l'utilisateur pour les ordinateurs prestataires.

L'authentification de la machine consiste à vérifier que celle-ci dispose bien d'un certificat valide alors que l'authentification de l'utilisateur consiste à vérifier que ce dernier est bien connu du serveur Active Directory.

Afin de garantir un niveau de sécurité certain, mon choix pour les méthodes est le suivant :

- Pour l'authentification machine, j'utiliserai la méthode EAP-TLS basée sur un certificat (cas d'un téléphone ou d'un ordinateur SVF),
- Pour l'authentification utilisateur, j'utiliserai la méthode PEAP/EAP MS-CHAP V2 basée sur un couple login/mot de passe (cas d'un ordinateur prestataire).

11.3. Récapitulatif des méthodes d'authentification retenues

Après l'étude des différents éléments à authentifier les méthodes retenues sont les suivantes :

Tableau X: Méthodes retenues par système.

TYPE	Méthodes d'authentification
PC SVF sous Windows XP	EAP-TLS
Téléphone IP	EAP-TLS
PC prestataires	PEAP/EAP MS-CHAP V2
Imprimante	Adresse Mac
Caméra IP	Adresse Mac
Équipements de GTB	Adresse Mac
Badgeuse	Adresse Mac
Visioconférence	Adresse Mac

12. Utilisation de VLAN spécifiques

L'un des intérêts de l'utilisation de VLAN pour la segmentation d'un réseau est qu'elle permet de regrouper des équipements en un ensemble logique isolé afin d'améliorer la sécurité.

Dans le cas présent, si un équipement de Sphéria Val de France se connecte avec succès, il se verra placé dans le vlan qui lui correspond (VLAN PC pour les ordinateurs, VLAN ToIP pour les téléphones).
Si un ordinateur n'appartenant pas à Sphéria Val de France se connecte avec succès, il se retrouvera dans un VLAN particulier n'ayant accès qu'à internet.
Par contre si une machine, qu'elle appartienne ou pas à Sphéria, obtient un refus de connexion, elle sera placée dans un VLAN de quarantaine ne disposant d'aucun accès.

Dans le cadre de la refonte du réseau Sphéria, les VLAN suivants avaient été créés permettant une segmentation des équipements par étage ou par fonction :

Tableau XI: VLAN en production.

Nom de VLAN	N° de VLAN	Description
Data-Utilisateurs-0	202	Réseau PC RDC
Data-Utilisateurs-1	212	Réseau PC 1er étage
Data-Utilisateurs-2	222	Réseau PC 2ème étage
Data-Utilisateurs-3	232	Réseau PC 3ème étage
Data-Utilisateurs-4	242	Réseau PC 4ème étage
Data-Utilisateurs-5	252	Réseau PC 5ème étage
Data-Utilisateurs-6	262	Réseau PC 6ème étage
Voix-Utilisateurs-0	702	Réseau ToIP RDC et Sous-sol
Voix-Utilisateurs-1	712	Réseau ToIP 1er étage
Voix-Utilisateurs-2	722	Réseau ToIP 2ème étage
Voix-Utilisateurs-3	732	Réseau ToIP 3ème étage
Voix-Utilisateurs-4	742	Réseau ToIP 4ème étage
Voix-Utilisateurs-5	752	Réseau ToIP 5ème étage
Voix-Utilisateurs-6	762	Réseau ToIP 6ème étage
Imprimantes	140	Réseau pour les imprimantes
Vidéosurveillance	180	Réseau pour les caméras IP
GTB	185	Réseau pour les équipements de GTB et les badgeuses

Pour la mise en place du 802.1x, deux nouveaux VLAN sont créés pour répondre aux besoins du projet :

Tableau XII: VLAN créés pour le 802.1x.

Nom de VLAN	N° de VLAN	Description
Guest-Internet	300	Réseau invité
Quarantaine	999	Réseau en cas d'échec d'authentification

Le but est de limiter l'impact sur l'architecture réseau existante et fonctionnelle mais de traiter le cas des machines dites « invité » et le cas des machines ayant échoué à s'authentifier.

Des listes de contrôles seront positionnées sur le cœur de réseau pour encadrer les flux du VLAN 300.

Un mécanisme de détection d'échec d'authentification doit être mis en place afin que les équipes informatiques soient informées très rapidement et puissent diagnostiquer s'il s'agit d'un problème ou d'une tentative d'intrusion.

Les schémas suivants résument l'attribution du VLAN en fonction de la méthode d'authentification et du résultat de celle-ci :

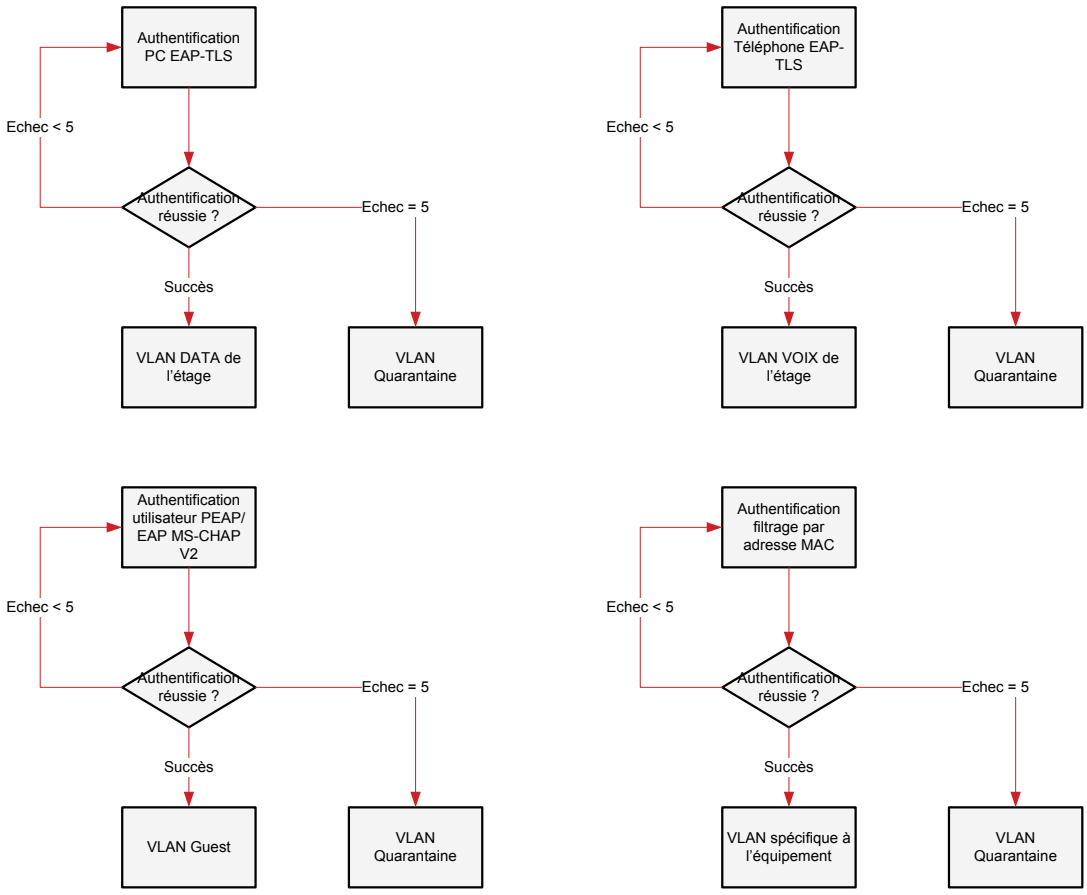


Figure 34: Affectation des VLAN.

13. Utilisation d'Access Control List (ACL)

Les listes de contrôle sont des règles qui permettent de filtrer les flux réseau, dans le cas présent il s'agit de n'autoriser que les flux nécessaires à l'authentification et la navigation

internet pour les ordinateurs des prestataires. Tout autre trafic se verra bloqué. Ces listes seront appliquées au VLAN Guest (VLAN 300).

14. Présentation et mise en place de la maquette

14.1. Description de la maquette

L'objectif de cette étape est de réaliser une maquette de l'architecture envisagée afin de tester les options techniques retenues et ensuite de créer les différentes procédures :

- Installation d'un équipement à filtrer par adresse MAC,
- Migration d'un équipement non 802.1x vers un filtrage par adresse MAC,
- Installation d'un ordinateur avec une authentification machine EAP-TLS,
- Migration d'un ordinateur vers une authentification machine EAP-TLS,
- Installation d'un téléphone IP avec une authentification EAP-TLS,
- Migration d'un téléphone IP vers une authentification EAP-TLS,
- Installation d'un ordinateur avec une authentification utilisateur PEAP/EAP MS-CHAP V2.

La maquette mise en place pour réaliser les tests est la suivante :

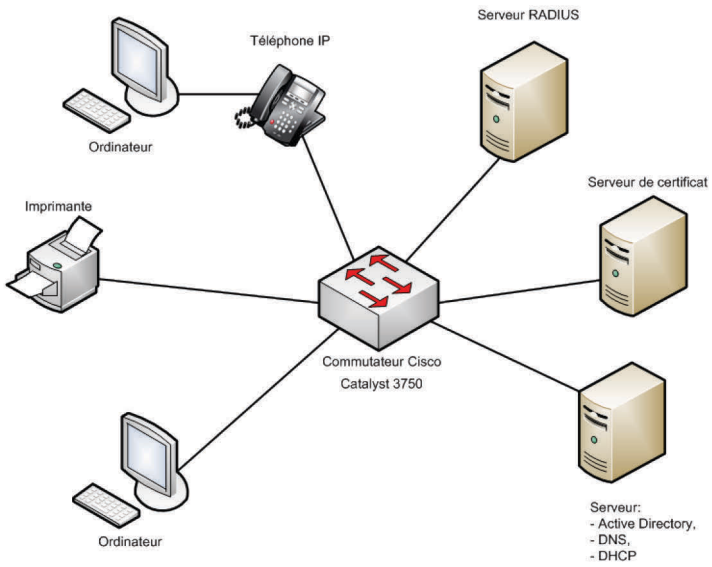


Figure 35: Maquette 802.1x.

Elle est constituée :

- Dans le rôle des systèmes à authentifier :
  - d'un ordinateur sous Windows XP Professionnel,
  - d'un téléphone IP Alcatel Intouché 4028,
  - d'une imprimante,
- Dans le rôle du système authentificateur : un commutateur Catalyst Cisco 3750,
- Dans le rôle du serveur d'authentification : un serveur Cisco 1120 ACS 5.1.0.44,
- D'un serveur Microsoft Windows 2003 Server avec Active Directory, service DNS et service DHCP,
- D'un serveur de certificat Microsoft Windows 2003 Server pour l'authentification EAP-TLS,
- D'un compte AD de test pour l'authentification PEAP/EAP MS-CHAP V2.

Cette maquette permet de tester les différentes méthodes d'authentification envisagées :

- Authentification machine EAP-TLS : ordinateurs SVF et téléphones IP,
- Authentification utilisateur PEAP/EAP MS-CHAP V2 : ordinateurs prestataires,
- Filtrage par adresse MAC : imprimante, caméra IP, équipements de GTB, visioconférences.

Limitations de la maquette :

Dans le cadre de la maquette il n'est pas possible de tester les visioconférences, les caméras IP ou les modules de Gestion Technique du Bâtiment (GTB) car ces équipements sont tous en production. Cependant comme ces équipements seront authentifiés par leur adresse MAC comme les imprimantes, il sera possible d'extrapoler les résultats.

14.2. Paramétrage des systèmes authentificateurs[5]

Le paramétrage a consisté à :

- Créer les nouveaux VLAN Guest et Quarantaine,
- Créer les ACL pour le VLAN Guest,
- Paramétrer les ports du commutateur en 802.1x,

[5] Annexe 12.

- Associer le commutateur avec le serveur RADIUS.

Le paramétrage détaillé ainsi que les explications associées se trouvent en annexe 12 de ce document.

14.3. Paramétrage du serveur d'annuaire[6]

Le paramétrage ici a consisté à créer :

- Un groupe Guest,
- Un groupe pour les ordinateurs,
- Les stratégies pour le déploiement des certificats ordinateurs,
- Les stratégies pour la configuration des cartes réseaux des ordinateurs.

Le paramétrage détaillé ainsi que les explications associées se trouvent en annexe 14 de ce document.

14.4. Paramétrage du serveur RADIUS[7]

Le paramétrage a consisté à :

- Créer et configurer les groupes,
- Associer les systèmes authentificateurs avec le serveur,
- Créer des comptes utilisateurs,
- Référencer les adresses MAC valides pour le filtrage par adresse MAC,
- Associer la base Active Directory au serveur ACS,
- Déclarer l'autorité de certification dans le serveur,
- Configurer le profil d'authentification par certificat,
- Configurer les profils d'autorisation,
- Configurer les règles d'accès,
- Activer les méthodes d'authentification : EAP-TLS, PEAP/EAP MS-CHAP V2,
- Paramétrer les rapports d'audit et les alertes qui seront envoyés au support.

[6] Annexe 14.
[7] Annexe 13.

Le paramétrage détaillé ainsi que les explications associées se trouvent en annexe 13 de ce document.

14.5. Paramétrage du serveur de certificat

Il n'y a pas de paramétrage proprement dit du serveur de certificat mais plutôt le choix des types de certificats qui vont être utilisés pour les ordinateurs et les téléphones :

- De type machine pour les ordinateurs,
- De type utilisateur pour les téléphones.

Etant donné que le parc ordinateur est renouvelé tous les trois ans et que le parc téléphonique est amorti sur cinq ans, le groupe projet a décidé d'utiliser des certificats valides pour une durée de six ans afin de simplifier la gestion des certificats notamment car les certificats pour les téléphones nécessitent une installation manuelle.

Figure 36: Trames utilisées pour les certificats.

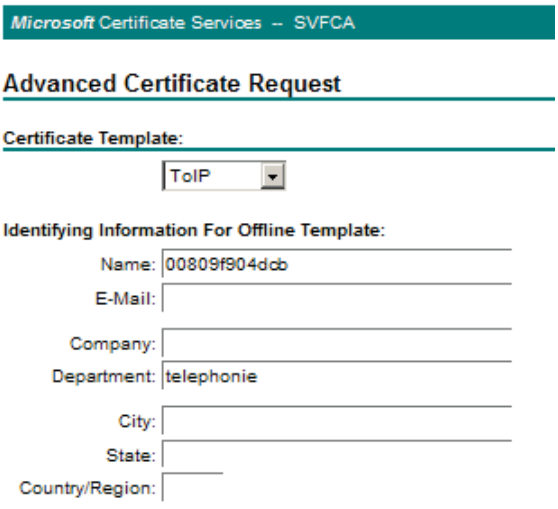


Figure 37: Exemple de requête de certificat pour un téléphone.

Un certificat est également installé sur chaque serveur RADIUS pour la communication avec l'autorité de certification.

14.6. Paramétrage des systèmes à authentifier

14.6.1. Paramétrage des ordinateurs SVF[8]

Le paramétrage a consisté à :

- Installer le certificat machine sur l'ordinateur,
- Paramétrer la carte réseau en EAP-TLS.

Le paramétrage détaillé ainsi que les explications associées se trouvent en annexe 9 de ce document.

14.6.2. Paramétrage des ordinateurs Prestataires[9]

Le paramétrage a consisté à :

- Paramétrer la carte réseau en PEAP/EAP MS-CHAP V2.

Le paramétrage détaillé ainsi que les explications associées se trouvent en annexe 9 de ce document.

14.6.3. Paramétrage des téléphones IP[10]

Le paramétrage a consisté à :

- Installer le certificat sur le téléphone,
- Activer l'authentification EAP-TLS sur le téléphone.

Le paramétrage détaillé ainsi que les explications associées se trouvent en annexe 11 de ce document.

[8] Annexe 9.
[9] Annexe 9.
[10] Annexe 11.

14.7. Phase de tests

Deux phases de tests ont été réalisées, la première phase utilisant un ordinateur seul comme client 802.1x et la seconde utilisant un téléphone IP seul comme client 802.1x.

Dans la première phase, 8 tests différents sont réalisés. Ces tests sont basés sur 8 scenarios possibles d'accès au réseau de Sphéria en faisant varier trois paramètres :

- Le mode d'authentification de la carte réseau de l'ordinateur : « mode **Machine »** ou « mode **Normal** »,
- Le certificat utilisé : « certificat de type **PC** » ou « certificat de type **téléphone** »,
- Le magasin où est stocké le certificat : « Magasin Personnel pour le compte **Utilisateur** » ou : « Magasin Personnel pour **l'ordinateur local** ».

14.7.1. Résultats des tests

L'ordinateur utilisé est la machine SVF510.

Le téléphone utilisé est le téléphone IP générique Alcatel utilisé chez Sphéria.

Le certificat PC est au nom de la machine SVF510.groupe.svf.fr.

Le certificat téléphone dans la première phase est associe à l'adresse MAC 6680.9f91.cd66

Voici les résultats des tests réalisés à partir d'un ordinateur SVF :

Tableau XIII : Résultats des tests pour un ordinateur SVF.

Test	AuthMode	Certificat utilisé	Certificat placé dans le magasin	Résultat	UsernameRadius
Test 1	Machine	PC	Ordinateur local	Succès	host/SVF510….
Test 2	Machine	PC	Utilisateur local	Échec / pas d'échange EAP	
Test 3	Machine	Téléphone	Ordinateur local	Échec	host/66809f91cd66
Test 4	Machine	Téléphone	Utilisateur local	Échec / pas d'échange EAP	
Test 5	Normal	PC	Ordinateur local	Échec / pas d'échange EAP	
Test 6	Normal	PC	Utilisateur local	Échec	SVF510…..
Test 7	Normal	Téléphone	Ordinateur local	Échec / pas d'échange EAP	
Test 8	Normal	Téléphone	Utilisateur local	Succès	66809f91cd66

Pour les tests de cette phase, avec la configuration actuelle de réseau Sphéria (configuration des commutateurs et de l'ACS), on voit que le test 1 représentant l'utilisation légitime d'un certificat PC aboutit à un succès mais que le test 8 représentant une utilisation frauduleuse d'un certificat téléphone installé sur un ordinateur aboutit également à un succès.
On note donc pour les cas de tentative de fraude, que seul le scénario où le certificat téléphone est placé dans le magasin personnel de l'utilisateur local aboutit à un succès (test 8).

On note également que pour qu'un échange EAP-TLS ait lieu, il faut que le certificat soit placé dans le magasin correspondant au mode d'authentification de la carte réseau :

- Si la carte est en **AuthMode=Machine** alors le certificat devra être placé dans le magasin personnel du compte **Ordinateur local**,

- Si la carte est en **AuthMode=Normal** (par défaut) alors le certificat devra être place dans le magasin personnel du compte **Utilisateur local**.

Voici le résultat du test réalisé à partir d'un téléphone SVF :

Tableau XIV : Résultat des tests pour un téléphone SVF.

Test	Certificat utilisé	Résultat	UsernameRadius
Test 1	Téléphone	Succès	ALCIPT

Pour le test de cette seconde phase, le but était de connaître la valeur de l'attribut UsernameRadius utilisé pour l'authentification d'un téléphone IP. On voit que la valeur utilisée est « ALCIPT ». C'est le paramètre que l'on utilisera pour distinguer l'authentification d'un téléphone légitime de l'authentification illégitime d'un ordinateur utilisant frauduleusement un certificat téléphone.

Bilan

Les résultats de ces tests montrent une faille concernant l'utilisation frauduleuse d'un certificat téléphone sur un ordinateur et donnent des informations sur l'attribut UsernameRadius utilisé pour les échanges avec le serveur ACS. Ces informations ont donc été utilisées pour modifier les règles[11] **Identity** et **Authorization Profile** sur l'ACS, afin d'interdire la connexion d'un ordinateur utilisant le certificat d'un téléphone.

14.7.2. Modifications apportées suite aux tests

La faille de sécurité qui avait été mise en évidence reposait sur le fait qu'un certificat téléphone installé sur un ordinateur de SVF dans le magasin personnel du compte Utilisateur avec la carte réseau en mode « Normal » constituait un scénario valide d'accès au réseau et représentait donc une utilisation frauduleuse et illégitime des certificats SVF.

La méthode retenue pour se prémunir contre cette faille est de modifier les règles du serveur ACS pour faire en sorte de distinguer la tentative de connexion d'un ordinateur utilisant un certificat PC (connexion légitime) d'une tentative de connexion d'un ordinateur utilisant un certificat téléphone (connexion illégitime).

[11] Annexe

Le principe de cette modification repose sur l'identification de manière unique d'un ordinateur légitime et d'un téléphone légitime en utilisant les attributs Radius envoyés lors de la phase d'authentification (du commutateur vers le serveur ACS).

Les tests d'authentification 802.1x par certificats ont montré qu'un téléphone utilise comme attribut UsernameRadius la chaine de caractères « **ALCIPT** ».

L'ordinateur, quel que soit le certificat installé, utilise lui comme attribut UsernameRadius la chaine de caractère « **host/SVFxxx.groupe.svf.fr ».**

On crée alors deux nouvelles règles sur le serveur RADIUS dans la partie « Access Policies > Access Services > Default Network Access > Identity » :

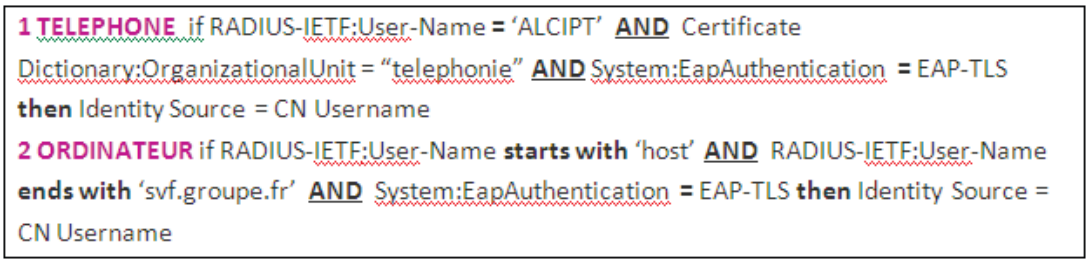


Figure 38: Nouvelles règles Identity.

Ces deux règles vont remplacer les deux règles existantes « toip » et « pc_tls ».

On crée deux autres règles dans la partie « Access Policies > Access Services > Default Network Access > Authorization » :

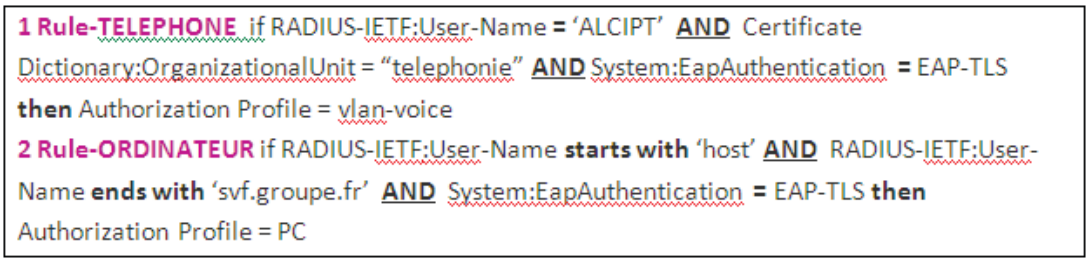


Figure 39: Nouvelles règles Authorization.

Ces deux règles vont remplacer les deux règles existantes « Rule-ToIP » et « Rule-PC ».
Des tests simples, basés sur l'incrémentation du compteur des règles et sur le verdict « Succès » ou « Échec » de l'authentification, montrent que ces nouvelles règles :

- Permettent bien les accès légitimes aux différents services du réseau (connexion ordinateur avec certificat légitime, connexion téléphone avec certificat légitime),
- Interdisent les accès illégitimes (connexion ordinateur avec certificat téléphone).

Ces nouvelles règles mises en place sur le serveur ACS permettent donc de protéger le réseau Sphéria des accès frauduleux d'ordinateurs avec des certificats de type téléphone.

14.8. Bilan de la phase de maquettage

A l'issue de la phase de maquettage qui a permis de tester les différentes méthodes d'authentification, j'ai pu répondre aux interrogations concernant les méthodes d'authentification retenues et la sécurisation du réseau.
Cette maquette a également permis de mettre en lumière des problématiques de sécurité concernant l'utilisation frauduleuse de certificats. La réponse apportée a été la modification des règles au niveau des serveurs RADIUS.
Cette phase a également permis de montrer la nécessité d'automatiser certaines parties du processus de migration étant donné le nombre important d'équipements à migrer.
La recette de l'automatisation des tâches suivantes sera donc réalisée lors du déploiement sur un périmètre restreint pour s'assurer de leur bon déroulement :

- Création des certificats Ordinateurs,
- Paramétrage de la carte réseau des ordinateurs concernés,
- Déploiement du certificat Ordinateur,
- Création des certificats Téléphone,
- Déploiement de la configuration sur les commutateurs.

Cette phase permettra également de valider les procédures de migration.

15. Déploiement

La phase de maquette m'ayant permis de m'assurer de la compatibilité des équipements avec les méthodes d'authentifications retenues, se pose désormais la question de la mise en

production de la solution. Le périmètre de déploiement se révélant relativement conséquent (plus de 780 équipements, tous types confondus), une mise en production en une fois représente un risque, des problèmes non identifiés pendant la phase de maquette pouvant survenir et dégrader la qualité du service.

En conséquence, le déploiement va se dérouler en plusieurs étapes. Une première phase sera réalisée sur un périmètre restreint, mais représentatif. Afin de minimiser l'impact sur les utilisateurs, mon choix s'est porté sur les équipements utilisés par les collaborateurs du Département Informatique (ordinateurs SVF, téléphones, équipements de GTB, imprimantes, caméras IP, visioconférence) ainsi la migration de ces équipements vers une authentification 802.1x peut être vérifiée et les éventuels problèmes identifiés.

A l'issue de cette étape, le planning définitif de migration des autres équipements sera établi et les notes d'informations concernant les coupures du réseau informatique seront préparées à destination des utilisateurs. Enfin la solution pourra être déployée sur le périmètre global.

15.1. Préparation du déploiement

La préparation du déploiement commence par un inventaire exhaustif des équipements qui devront être authentifiés. Ce recensement se décompose comme suit :

- 276 téléphones,
- 86 imprimantes réseau,
- 22 caméras IP,
- 2 visioconférences,
- 43 équipements de GTB,
- 352 ordinateurs.

La deuxième étape consiste à :

- Créer l'ensemble des certificats pour les téléphones IP (voir annexe 11),
- Mettre en place les GPO pour les ordinateurs (voir annexe 15),
- Importer les adresses MAC des imprimantes, caméras IP, visioconférences et équipements de GTB sur le serveur ACS (voir annexe 13).

15.1.1. Procédure de migration

Le schéma ci-dessous décrit les étapes à respecter pour la migration des équipements qui sont en production.

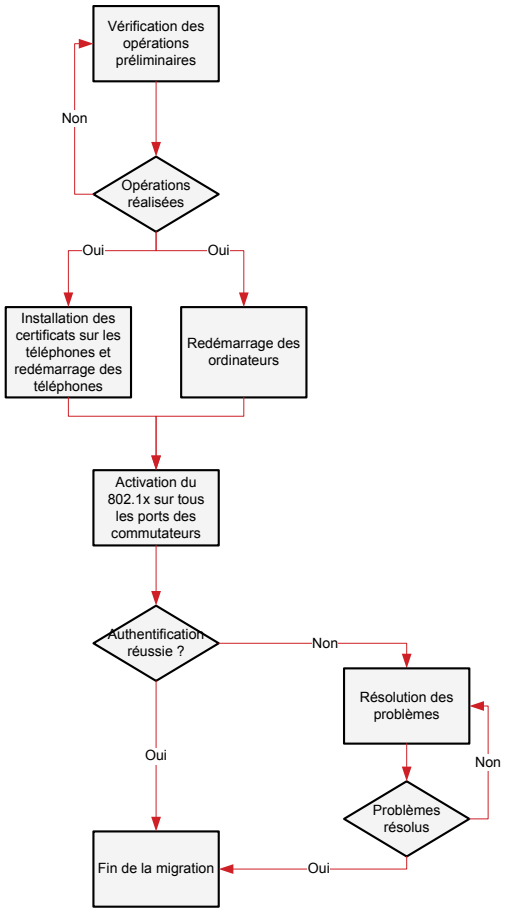


Figure 40: Procédure de migration des équipements.

15.1.2. Procédure d'installation d'un nouvel équipement

Pour l'installation d'un nouvel équipement la documentation existante a été amendée afin de tenir compte des spécificités liées au 802.1x. Les modes opérateurs des techniciens incluent désormais toutes les informations nécessaires au déploiement d'un équipement (quelque soit son type) dans un environnement 802.1x (voir annexe 18).

15.2. Déploiement sur un périmètre restreint

Le déploiement est réalisé sur le premier étage du bâtiment et uniquement sur les équipements utilisés par le DI SVF.
Le but de cette étape est d'appliquer la procédure de migration sur des équipements référents, de vérifier le bon fonctionnement de la solution durant deux semaines et de faire un bilan.

Problème rencontré : A l'issue du déploiement sont apparus des problèmes de déconnexions aléatoires des équipements clients (ordinateurs, badgeuses, …) nécessitant un redémarrage des équipements concernés ou une réactivation de l'interface réseau.

Solution : Notre consultant de l'entreprise Telindus a pu déterminer que cela était lié à une incompatibilité entre la fonctionnalité Port-security qui est activée sur tous les ports des commutateurs Sphéria et le 802.1x paramétré en mode multi-domain.
La commande Port-security était utilisée pour limiter le nombre d'équipements simultanés par interface de commutateur.
La configuration 802.1x en mode multi-domain quant à elle permet d'autoriser uniquement un équipement pour le VLAN Data et un équipement pour le VLAN Voix par interface, ce paramétrage étant indispensable puisque les ordinateurs sont connectés sur les téléphones eux-mêmes connectés aux commutateurs.

Bien que Cisco n'indique pas d'incompatibilité entre ces deux fonctions, il n'est pas recommandé de les activer simultanément sur une même interface.
Après désactivation de la fonction Port-security, les symptômes constatés ont alors disparu.

Bilan : hormis le problème lié à la fonction Port-security, par ailleurs résolu, l'architecture fonctionne. Il est donc possible de passer à la phase de déploiement sur le périmètre global.

15.3. Déploiement sur le périmètre global

Cette deuxième phase du déploiement ne présente pas de difficultés techniques particulières, les procédures ont été testées et validées précédemment. Cependant, étant donné l'architecture réseau du bâtiment, le nombre de matériels concernés et le caractère plus sensible de certains services, il est décidé de scinder le déploiement en deux étapes.

L'activation du 802.1x se fait par pile de commutateurs, une pile pouvant alimenter plusieurs étages du bâtiment.
Les interventions sont réalisées en heures non ouvrées à partir de 19h, en accord avec les différents services impactés.

15.3.1. Première étape

Le déploiement est réalisé le 22 septembre 2011 sur les étages suivants :

- Agence Jaurès (local LT0-JJ),
- Rez de chaussée (local LT1-JJ),
- Etage R+1 (local LT1-JJ),
- Amphithéâtre (local LT2-JJ),
- Etage R+2 et une partie de l'étage R+3 (locaux LT3-JJ et LT3-MT).

Tableau XV: Planning de migration de l'étape 1.

Local technique	Services	Sensibilité	Date
LT0-JJ	Agence Jaurès	Normale	22/09/2011
LT1-JJ	Accueil, Service social	Normale	22/09/2011
LT2-JJ	Amphithéâtre	Normale	22/09/2011
LT3-JJ	STA, Direction Commerciale, Services de Gestion	Normale	22/09/2011
LT3-MT	Développement, Marketing, Communication, Partenariat et Service, Centre de contacts	Normale	22/09/2011

Les notes d'informations sont communiquées aux utilisateurs des services concernés.

15.3.2. Seconde étape

Le déploiement est réalisé le 27 septembre 2011 sur les étages suivants :

- Etages R+4, R+5, R+6 (locaux LT4-MT et LT5-JJ) et fin de l'étage R+3 (local LT4-MT).

Tableau XVI: Planning de migration de l'étape 2.

Local technique	Services	Sensibilité	Date
LT4-MT	Direction des Ressources Humaines, Contrôle de Gestion, Comptabilité, Télévente	Haute	27/09/2011
LT5-JJ	Direction Générale, Direction Juridique, Présidence	Haute	27/09/2011

Les notes d'informations sont communiquées aux utilisateurs des services concernés.

16. Bilan

A l'issue de la mise en production qui s'est parfaitement déroulée, l'objectif du projet a été atteint car l'accès physique au réseau de l'entreprise est désormais sécurisé. L'identité des équipements désirant se connecter au réseau de Sphéria Val de France peut être vérifiée et il est également possible de détecter et de bloquer les tentatives d'intrusion.

Après une période de quelques jours il a toute fois été nécessaire de revoir légèrement les seuils de déclenchement des alertes Radius afin d'éliminer les faux positifs qui pouvaient apparaître.
Avec quelques mois de recul j'ai pu constater que dans le cadre d'interventions de prestataires, l'impact de la solution sur le fonctionnement organisationnel de l'entreprise n'était pas totalement assimilé. Il est donc nécessaire de rappeler de manière ponctuelle aux différents responsables de service la nécessité d'informer préalablement le Département Informatique de l'intervention de personnels extérieurs, conformément au processus de demande d'habilitation, afin de fournir les accès adéquats.

Les quelques cas de dysfonctionnement, lors du déploiement ou du remplacement d'un matériel, qui peuvent être rencontrés aujourd'hui sont plutôt le fait d'un oubli ou d'une mauvaise application des procédures de déploiement.

La solution mise en œuvre se révèle très stable et parfaitement fonctionnelle.

17. Perspectives d'évolution

Comme je l'ai indiqué précédemment les besoins initiaux sont couverts par la solution déployée. Cependant, de nouveaux besoins commencent à apparaitre et il est toujours possible d'améliorer l'infrastructure mise en place afin de renforcer encore la sécurité.

17.1. Déploiement sur de nouveaux sites du groupe

A l'issue de ce projet et étant donné les résultats obtenus, une réflexion pour étendre l'utilisation du protocole 802.1x à l'ensemble des sites du groupe va être menée.
Il faudra, entre autre, s'assurer que les commutateurs de ces sites sont compatibles 802.1x et supportent l'outre passement de l'authentification en cas de défaillance des serveurs RADIUS présents sur le site d'Orléans Jaurès. La question de l'intégration d'un serveur RADIUS sur le site de PRA sera également à étudier.

17.2. Renforcement de la sécurité

Il serait intéressant de renforcer la sécurité par la notion d'intégrité machine, principalement en se donnant la possibilité de vérifier la présence d'un logiciel antivirus à jour sur le poste client ou la version du système d'exploitation.

17.3. Sécurisation de l'accès internet

Pour des raisons budgétaires et par rapport à la faible population concernée, le choix avait été fait concernant les accès « Prestataires internet » d'utiliser des ACL sur le cœur de réseau.
Il pourrait désormais être envisagée la mise en place d'une solution de portail captif de type Ucopia qui, outre le fait qu'elle permettrait de se substituer à ces ACL, assurerait également une traçabilité et une conservation des données de connexion qu'impose la législation.

Cette solution ne nécessiterait plus de paramétrage particulier sur les ordinateurs des prestataires. De plus elle serait parfaitement adaptée en prévision de la mise en place d'un réseau wifi au sein de Sphéria Val de France.
L'investissement s'élèverait à 7 600 €HT.

Conclusion

La Direction du groupe Sphéria Val de France souhaitait améliorer la sécurité de son réseau informatique en s'assurant de l'identité des ordinateurs accédant à son Système d'Information.
Une analyse exhaustive des besoins et des contraintes de l'entreprise, qui a souligné la difficulté de sécuriser l'accès au réseau local, m'a conduit à la conclusion que seule l'utilisation du protocole 802.1x permettait de répondre à la problématique.

Partant de l'état de l'art, j'ai dû choisir des méthodes d'authentification en cohérence avec le système d'information existant, en tenant compte notamment des spécificités des différents matériels à authentifier.
La phase de maquette, en plus de me permettre de valider les orientations techniques, a permis de montrer qu'une utilisation frauduleuse de certificats était possible si les règles du serveur RADIUS n'étaient pas très précisément définies.
Le déploiement sur le périmètre restreint s'est révélé très utile pour déceler les problèmes non apparents en maquette et valider les procédures de migration.
Sphéria Val de France dispose désormais d'une solution très stable, fonctionnelle et qui au quotidien ne nécessite pas une charge d'exploitation ou d'administration importante. De plus elle est parfaitement évolutive.

La réalisation de ce projet a été très enrichissante que ce soit au niveau technique par la découverte du protocole 802.1x et des différentes technologies mises en œuvre, mais aussi au niveau de la gestion d'un projet. J'ai été amené à gérer une équipe, animer des réunions et arrêter la meilleure solution répondant aux besoins de SVF. Loin de devoir me focaliser sur des questions purement techniques, il m'a été nécessaire de prendre du recul afin d'avoir une vision globale pour bien prendre en compte les contraintes de l'entreprise et mesurer les impacts des choix à faire. La bonne conduite d'un projet est exigeante en termes d'organisation et de communication.
La réalisation de ce mémoire a été une occasion plus particulière de mettre en application les connaissances acquises au CNAM.

Pour conclure ce mémoire je souhaiterais rajouter qu'il faut garder à l'esprit que la sécurité totale n'existe pas. Il s'agit d'un compromis entre les contraintes qui peuvent être supportées

par l'entreprise et les bénéfices qu'elle peut en retirer, son efficacité devant sans cesse être remise en question.

Table des annexes

Annexe 1 RFC (Request For Comments) **90**
Annexe 2 Compte rendu de réunion : Présentation du projet **91**
Annexe 3 Compte rendu de réunion : Présentation des solutions techniques possibles **92**
Annexe 4 Compte rendu de réunion : Présentation de la solution technique retenue **93**
Annexe 5 Compte rendu de réunion : Définition des tests pour la VABF **94**
Annexe 6 Compte rendu de réunion : Mise en production sur des équipements référents **95**
Annexe 7 Compte rendu de réunion : Bilan de l'intégration des équipements référents **96**
Annexe 8 Compte rendu de réunion : Planning de migration **97**
Annexe 9 Configuration des ordinateurs **98**
Annexe 10 Script de configuration de la carte réseau d'un ordinateur SVF **103**
Annexe 11 Configuration des téléphones **104**
Annexe 12 Configuration des commutateurs et des ACL **107**
Annexe 13 Configuration des serveurs ACS **110**
Annexe 14 Configuration du serveur d'annuaire **120**
Annexe 15 Configuration des GPO **121**
Annexe 16 Exemple d'échanges lors d'une authentification 802.1x pour un ordinateur SVF **122**
Annexe 17 Processus de traitement des requêtes 802.1x par le serveur ACS **123**
Annexe 18 Procédures de déploiement des nouveaux matériels **124**

Annexe 1
RFC (Request For Comments)

Radius

- RFC 2865 : Remote Authentication Dial In User Services (Radius) ;

Radius et EAP

- RFC 2869 : Radius Extensions ;
- RFC 3579 : Radius Support for Extensible Authentication Protocol (EAP) ;
- RFC 2868 : Radius Attributes for Tunnel Support ;
- RFC 4137 : State machine for Extensible Authentication Protocol (EAP) ;
- RFC 3748 : Extensible Authentication Protocole (EAP) ;
- RFC 3580 : IEEE 802.1X Remote Authentication Dial In User Services (radius) Usage Guidelines.

TLS

- RFC 4346 : The Transport Layer Security (TLS) Protocol Version 1.1 ;
- RFC 4366 : Transport Layer Security (TLS) Extensions ;
- RFC 2716 : PPP EAP TLS Authentication Protocol.

PEAP

- Protected EAP Protocol (PEAP) Version 2. http://ietfreport.isoc.org/all-ids/draft-josefsson-pppext-eap-tls-eap-10.txt

LDAP

- RFC 2251 : Lightweight Directory Access Protocol (LDAP).

Certificats X509

- RFC 3280 : Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

Annexe 2
Compte rendu de réunion : Présentation du projet

Date : 4 mai 2011

Participants : Responsable du DI, Responsable SIT, Responsable Service Projet, Ingénieur Sécurité, Ingénieur Système, Consultant Telindus, Chef de projet.

Objet de la réunion :

- Présentation du projet de sécurisation de l'accès au réseau local de Sphéria Val de France »,
- Constitution de l'équipe projet.

Besoins :

- Autoriser ou refuser l'accès d'un équipement au réseau informatique de SVF sur le site Orléans Jaurès,
- Détecter les tentatives d'intrusion.

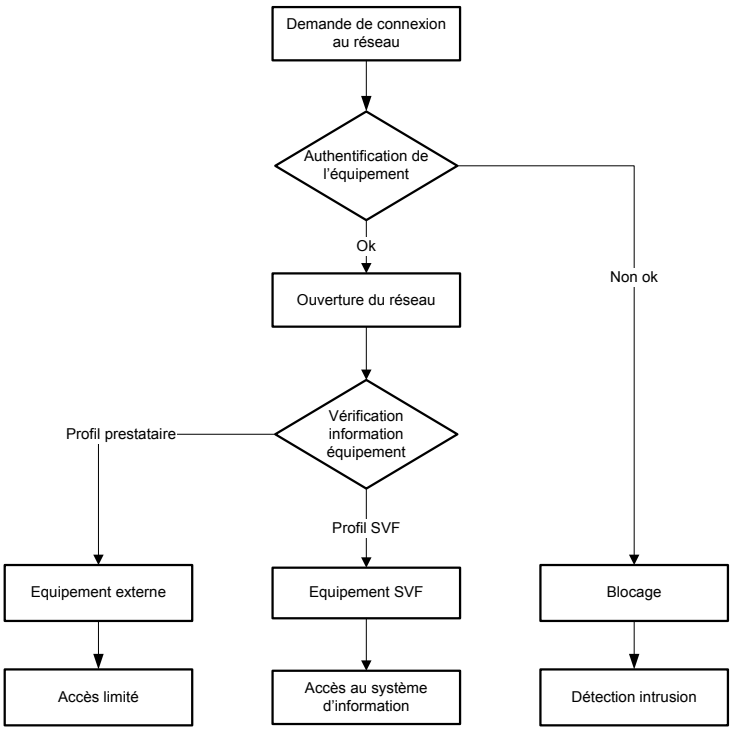


Figure 41: Processus d'authentification.

Annexe 3
Compte rendu de réunion : Présentation des solutions techniques possibles

Date : 20 juin 2011

Participants : Responsable du DI, Responsable SIT, Responsable Service Projet, Ingénieur Sécurité, Ingénieur Système, Consultant Telindus, Chef de projet.

Objet de la réunion :

- Présentation des solutions techniques possibles,
- Orientation des choix techniques.

Questions :

- Quel mode d'authentification pour les équipements 802.1x : Certificats ou filtrage des adresses MAC,
- Quelle solution pour les prestataires : ordinateur de prêt ou ordinateur personnel,
- Comment seront déployés les certificats ordinateurs : manuellement ou par GPO,
- Comment peut-on intégrer les certificats sur les téléphones IP ?

Réponses :

- L'authentification des équipements 802.1x se fera par certificat,
- Les prestataires n'ayant besoin d'accéder qu'à internet pourront utiliser leur ordinateur, dans les autres cas un ordinateur sera fourni par SVF,
- Les certificats pour les ordinateurs seront déployés par GPO,
- Les certificats pour les téléphones devront être intégrés manuellement sur les téléphones.

Annexe 4
Compte rendu de réunion : Présentation de la solution technique retenue

Date : 27 juin 2011

Participants : Responsable du DI, Responsable SIT, Responsable Service Projet, Ingénieur Sécurité, Ingénieur Système, Consultant Telindus, Chef de projet.

Objet de la réunion : Présentation de la solution technique retenue.

Solution technique :

- Pour les équipements SVF (ordinateurs et téléphones) : authentification machine EAP-TLS,
- Pour les équipements ne gérant pas le 802.1x : filtrage par adresse MAC,
- Pour les prestataires devant accéder au SI : prêt d'un ordinateur SVF,
- Pour les prestataires avec accès internet uniquement : possibilité d'utiliser leur ordinateur personnel, utilisation d'un vlan spécifique et authentification utilisateur EAP/PEAP MS-CHAP V2.

Moyens :

- Pour l'authentification : utilisation de serveurs RADIUS Cisco ACS,
- Pour la méthode EAP-TLS : utilisation d'une autorité de certification,
- Utilisation de vlan quel que soit le résultat de l'authentification (voir tableau ci-dessous)

Tableau XVII : Nouveaux vlan pour le 802.1x.

Nom de VLAN	N° de VLAN	Description
Guest-Internet	300	Réseau invité
Quarantaine	999	Réseau en cas d'échec d'authentification

Annexe 5
Compte rendu de réunion : Définition des tests pour la VABF

Date : 29 juin 2011

Participants : Responsable du DI, Responsable SIT, Responsable Service Projet, Ingénieur Sécurité, Ingénieur Système, Chef de projet

Objet de la réunion : Définir les tests qui seront réalisés pour la VABF.

Tests retenus :

- Test de reprise d'activité du serveur ACS de secours,
- Test de simulation de connexion prestataires,
- Test de connexion imprimante,
- Test de connexion d'un ordinateur SVF.

Annexe 6
Compte rendu de réunion : Mise en production sur des équipements référents

Date : 29 août 2011

Participants : Responsable du DI, Responsable SIT, Responsable Service Projet, Ingénieur Sécurité, Ingénieur Système, Responsable CSI, Chef de projet.

Objet de la réunion : Présentation de la phase de déploiement sur des équipements référents.

But : Valider la solution technique et les procédures de migration.

Annexe 7
Compte rendu de réunion : Bilan de l'intégration des équipements référents

Date : 9 septembre 2011

Participants : Responsable du DI, Responsable SIT, Responsable Service Projet, Ingénieur Sécurité, Ingénieur Système, Responsable CSI, Chef de projet.

Objet de la réunion :

- Bilan de l'intégration,
- Présentation du processus de déploiement sur l'ensemble du site,
- Présentation du mode de déploiement pour tout futur équipement (post migration).

Bilan : Problème d'incompatibilité entre le 802.1x et la fonction Port-security sur les commutateurs entrainant des pertes de connexion.
La désactivation de la commande Port-security a résolu le problème.

Annexe 8
Compte rendu de réunion : Planning de migration

Date : 14 septembre 2011

Participants : Responsable du DI, Responsable SIT, Responsable Service Projet, Responsable CSI, Chef de projet.

Objet de la réunion : Présenter et valider le planning de migration

Déploiement sur l'ensemble du site :

- Le déploiement sera réalisé en deux étapes :
    - Rez de chaussée, R+1, R+2 et R+3 le 22 septembre,
    - R+4, R+5, R+6 le 27 septembre,
- L'ensemble des certificats téléphones a été généré,
- L'ensemble des ordinateurs concernés se voit déjà appliquer les GPO de configuration de la carte réseau et d'installation du certificat ordinateur,
- Informer les membres de la Direction Générale et les responsables de services sensibles (RH, Juridique, …) du passage dans les bureaux pour intervention en heures non ouvrés. Leur proposer aussi que l'intervention ait lieu en leur présence en journée.
- Fourniture d'un accès en lecture seule au CSI aux rapports d'audit des serveurs RADIUS et destinataire des alertes emails.

Mode de déploiement pour tout futur équipement :

- La fiche d'habilitation existante sera utilisée pour les demandes d'accès des prestataires,
- Mise à jour des procédures existantes de déploiement de matériel en intégrant le paramétrage 802.1x

Annexe 9
Configuration des ordinateurs

Configuration des ordinateurs SVF

Script de configuration automatique de la carte réseau

Pour configurer la carte réseau d'un ordinateur afin qu'elle soit compatible 802.1x, il faut au préalable que le service « Configuration de réseau câblé » soit démarré automatiquement. Ce service permet d'avoir accès à la configuration 802.1x de la carte réseau. On y définit la méthode d'authentification (certificat), ainsi que l'autorité de certification (SVFCA).

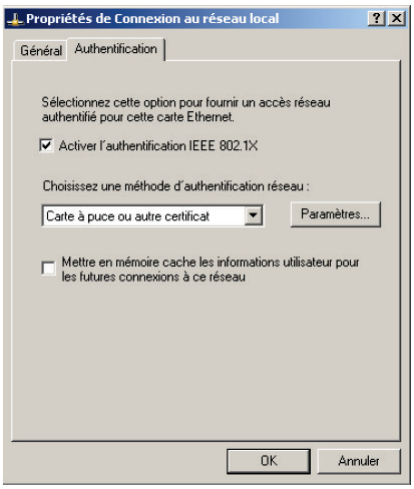


Figure 42: Activation de l'authentification et choix de la méthode.

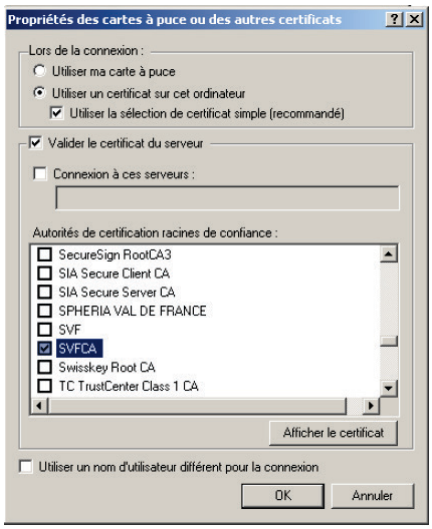


Figure 43: Sélection du certificat.

Une fois la configuration faite, il convient de l'exporter à l'aide de cette commande :

```
C:\>netsh lan export profile folder=c:\
```

Figure 44: Commande d'export de la configuration de la carte réseau.

Le fichier de configuration obtenu est au format XML :

```
<?xml version="1.0" ?>
<LANProfile xmlns="http://www.microsoft.com/networking/LAN/profile/v1">
<MSM>
<security>
<OneXEnforced>false</OneXEnforced>
<OneXEnabled>true</OneXEnabled>
<OneX xmlns="http://www.microsoft.com/networking/OneX/v1">
<cacheUserData>false</cacheUserData>
<authMode>machine</authMode>
<EAPConfig>
<EapHostConfig xmlns="http://www.microsoft.com/provisioning/EapHostConfig">
<EapMethod>
<Type xmlns="http://www.microsoft.com/provisioning/EapCommon">13</Type>
<VendorId xmlns="http://www.microsoft.com/provisioning/EapCommon">0</VendorId>
<VendorType xmlns="http://www.microsoft.com/provisioning/EapCommon">0</VendorType>
<AuthorId xmlns="http://www.microsoft.com/provisioning/EapCommon">0</AuthorId>
</EapMethod>
<ConfigBlob>020000002A000000150000107C7287E90129D66F47A56889A69D000001000000</ConfigBlob>
</EapHostConfig>
</EAPConfig>
</OneX>
</security>
</MSM>
</LANProfile>
```

Figure 45: Fichier de configuration de la carte réseau.

Par défaut, la configuration ira chercher le certificat dans le magasin de certificat utilisateur. Pour l'authentification des ordinateurs, on doit forcer la carte réseau à chercher dans le magasin de certificat ordinateur. Pour ce faire, j'ai ajouté la ligne suivante:

<authMode>machine**</authMode>**

La configuration est maintenant prête à être importée sur d'autres PC. Voici la commande :

```
C:\>netsh lan add profile filename="nomDuFichier.xml" interface="Connexion au réseau local"
```

Figure 46: Commande d'import de la configuration de la carte réseau.

Pour faciliter cette étape j'ai développé un script en Visual Basic qui permet l'importation du fichier XML. Ce script sera exécuté à partir de chaque PC SVF à l'aide de la GPO SVFGPO093 (Annexe 15).

Installation du certificat pour les ordinateurs

Pour récupérer le certificat afin d'être authentifié par l'ACS via la méthode EAP-TLS, il faut que l'ordinateur souhaité soit membre de ORLINFCENOPT 802.1X sur lequel est appliqué une GPO. Une fois cette action faite, il faut redémarrer l'ordinateur.

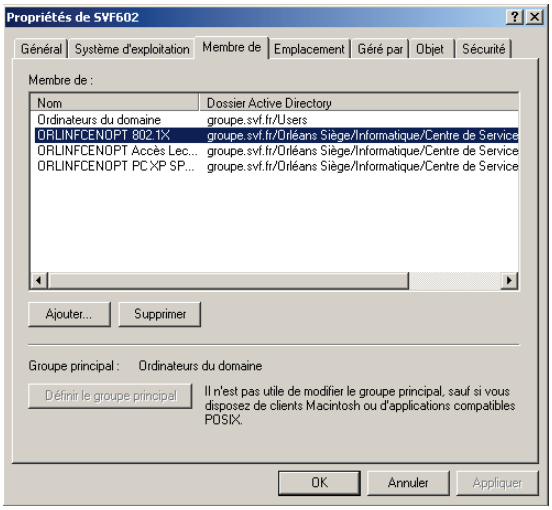


Figure 47: Groupe pour les ordinateurs 802.1x.

L'ordinateur une fois démarré devra posséder le certificat, afin de vérifier que le certificat a bien été correctement importé, il suffit d'ouvrir une console MMC et d'ajouter le composant enfichable « Certificats », de choisir l'option compte de l'ordinateur et de vérifier dans le répertoire personnel que le certificat portant le nom de la machine est délivré par l'autorité de certification est bien présent.

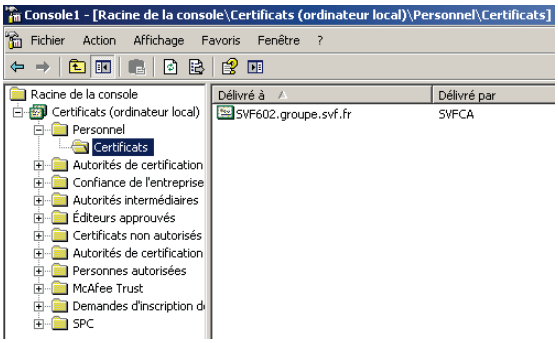


Figure 48: Vérification de la présence du certificat.

La durée de validité du certificat est de 1 an. Une période de 6 semaines avant la date d'expiration du certificat permet au PC d'effectuer sa demande de renouvellement de manière automatique. Ces paramètres sont définis dans la GPO SVFGPO084 (Annexe 15).

Configuration des ordinateurs Prestataires

La configuration du 802.1x et de la méthode EAP PEAP (Couple login/mot de passe pour accéder au réseau) sur les ordinateurs des prestataires se fait dans les propriétés de la connexion réseau local.

Dans l'éventualité où l'onglet authentification des propriétés de la connexion au réseau local, n'est pas présent, il faut activer le service: « configuration automatique de réseau câblé » puis mettre le service en démarrage automatique.

Dans ce dernier il est possible de définir l'activation du 802.1x.

Il faut cocher l'option « Activer l'authentification IEEE 802.1x pour ce réseau » puis sélectionner le type d'EAP « EAP protégé (PEAP) ». Puis, il faut cliquer sur l'onglet « Propriétés ».

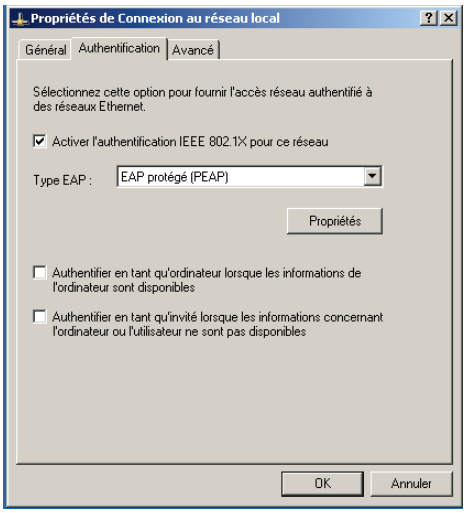


Figure 49: Activation de l'authentification sur un ordinateur prestataire.

Dans l'onglet « Propriétés », sélectionner la méthode d'authentification « Mots de passe sécurité (EAP-MSCHAP version 2) »

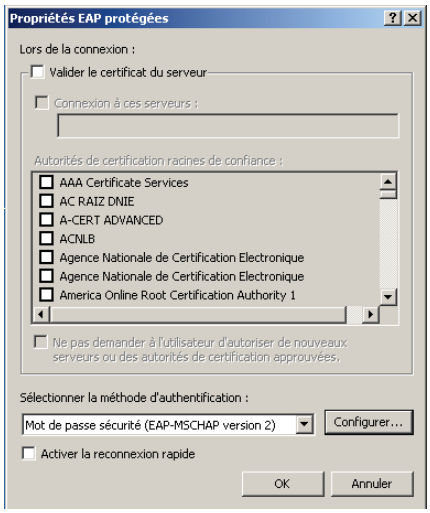


Figure 50: Choix de la méthode d'authentification.

Lors de l'activation du PEAP avec authentification via le couple login/mot de passe la fenêtre suivante s'affichera. Au clic, une fenêtre demandant d'entrer les informations d'authentification apparaîtra.

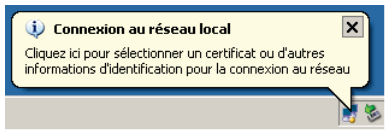


Figure 51: La connexion réseau nécessite une identification.

Il faudra entrer dans cette section les informations d'identification, c'est-à-dire le couple login/mot de passe communiqué au prestataire.

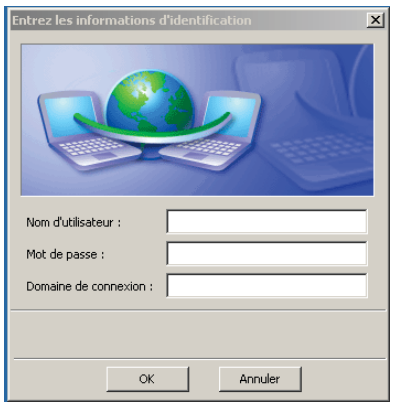


Figure 52: Saisie des informations d'identification.

Annexe 10
Script de configuration de la carte réseau d'un ordinateur SVF

```
Option Explicit
'On Error Resume Next
Dim objComputer, colComputer, strComputer2
Dim fso, file, WshShell, cptr, cptrok, i, path, profile, log, find
Dim cible,a,b,c,d,e,f
Dim IPConfigSet, objWMIService2, IPConfig, objWMIService
Dim oFSO
Dim oF, cherche, oExec, service_state
service_state = 0
Const ForReading = 1, ForWriting = 2

Set oFSO = CreateObject("Scripting.FileSystemObject")
Set fso = CreateObject("Scripting.FileSystemObject")
Set oF = CreateObject("Scripting.FileSystemObject")
Set WshShell = CreateObject("WScript.Shell")

strComputer2 = "localhost"
Set objWMIService2 = GetObject("winmgmts:\\" & strComputer2 & "\root\cimv2")
Set IPConfigSet = objWMIService2.ExecQuery("Select IPAddress, DNSHostName, MACAddress from Win32_NetworkAdapterConfiguration where IPEnabled=TRUE")
Set objWMIService = GetObject("winmgmts:" & "{impersonationLevel=impersonate}!\\" & strComputer2 & "\root\cimv2")
Set colComputer = objWMIService.ExecQuery("Select * from Win32_ComputerSystem")

'Recherche des variables d'identification de l'environnement
For Each IPConfig in IPConfigSet
        If Not IsNull(IPConfig.IPAddress) Then
                For Each objComputer in colComputer
                        If objComputer.UserName <> "" then
                                For i=LBound(IPConfig.IPAddress) to UBound(IPConfig.IPAddress)
                                        'Wscript.Echo Date & " " & Time & VBCRLF & IPConfig.DNSHostName(i) & VBCRLF & objComputer.UserName(i) & VBCRLF
                                         & IPConfig.IPAddress(i) & VBCRLF & IPConfig.MACAddress(i)
                                        a = Date
                                        b = Time
                                        c = IPConfig.DNSHostName(i) 'Nom du PC
                                        d = objComputer.UserName(i) 'Nom de l'utilisateur
                                        e = IPConfig.IPAddress(i)       'Adresse IP
                                        f = IPConfig.MACAddress(i)      'Adresse MAC
                                Next
                        else
                                For i=LBound(IPConfig.IPAddress) to UBound(IPConfig.IPAddress)
                                        'Wscript.Echo "FAIL ! " & IPConfig.IPAddress(i)
                                        a = Date
                                        b = Time
                                        c = IPConfig.DNSHostName(i) 'Nom du PC
                                        d = "nobody"                            'Nom de l'utilisateur
                                        e = IPConfig.IPAddress(i)       'Adresse IP
                                        f = IPConfig.MACAddress(i)      'Adresse MAC
                                Next
                        end if
                Next
        End If
Next

'Chemin où sera sauvegardé les logs et où est stocké le profil svf
        'path = "\\srv01dfs\reslog$\"
        'path = "\\srv01fic\commun$\deplnosuppr\"
path = "\\srv01vas\deplconfrez$\"

'variable contenant le nom du fichier de log
log = c & ".log"
'variable contenant le chemin du fichier de log
cible = path & log
'variable contenant le chemin du fichier de profile
profile = path & "svf.xml"

'Test si le profil svf existe puis si un log de la machine existe
If oFSO.FileExists(profile) Then
        If Not oFSO.FileExists(cible) Then
                'Si le log n'existe pas il est créé
                Set file = fso.OpenTextFile(cible, ForWriting,true)
                file.write(a & " " & b & VBCRLF & c & VBCRLF & d & VBCRLF & e & VBCRLF & f & VBCRLF)
                file.Close
        End If

        Set oExec = WshShell.Exec("cmd /c sc interrogate ""Dot3svc"" | find /c /i ""running""")
        service_state = CInt(oExec.StdOut.ReadAll)
        'Vérification si le service est bien lancé
        If service_state <> 1 Then
                'Wscript.Echo "service non lancé"

                'S'il ne l'est pas on le met en mode auto et on le lance
                'Wscript.Echo "dot3svc auto" '"start= auto" espace important
                WshShell.Run "cmd /C sc config Dot3svc start= auto",0,true

                'Wscript.Echo "lance dot3svc"
                WshShell.Run "cmd /C net start Dot3svc",0,true
        End If
        'Modification du profile de la carte réseau
        WshShell.Run "cmd /C  netsh lan add profile filename=""" & profile & """ interface=""Connexion au réseau local""",0,true
        WshShell.Run "cmd /C netsh lan show profile >> " & cible & "",0,true
        'Wscript.Echo "Configuration modifié"
else
        Wscript.Echo "no .xml"
End If
```

Figure 53: Script de configuration de la carte réseau.

Annexe 11
Configuration des téléphones

Script de génération des certificats pour les téléphones

L'installation d'un certificat sur les téléphones nécessite impérativement une intervention manuelle, Alcatel n'a pour l'instant pas développé de solution d'automatisation.

Dans le cas d'un déploiement important il est nécessaire de générer l'ensemble de ces certificats. Pour ce faire, on dispose de l'interface web de l'autorité de certification, qui permet de générer un à un les certificats.

Cette option n'étant pas adaptée à un déploiement de près de 280 certificats, j'ai créé un programme utilisant les requêtes de certificat en ligne de commande. Le problème qui s'est présenté à moi est le manque de documentations officielles de cette méthode, pour un environnement Windows.

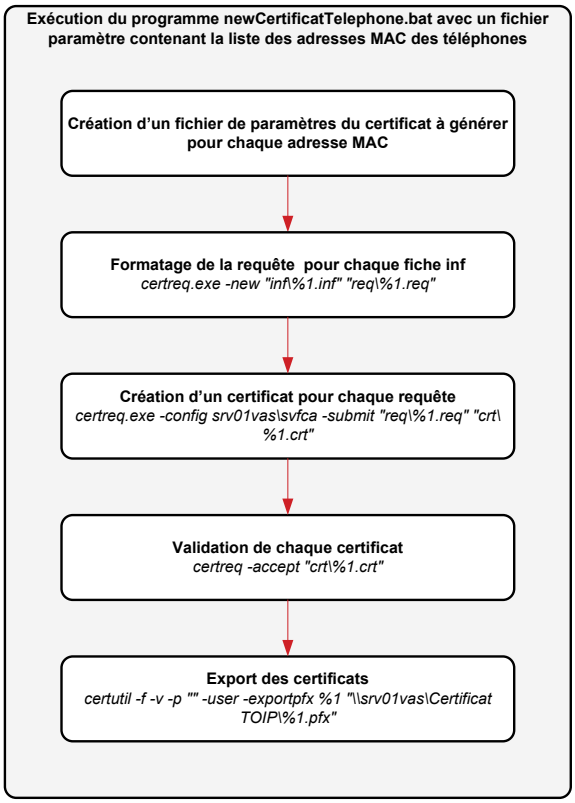


Figure 54: Logigramme du programme de génération des certificats téléphones.

Le programme prend en paramètre un fichier texte contenant une liste d'adresses MAC (une par ligne). Il génère un certificat sous la forme '@mac'.crt, en fonction de l'adresse MAC

passée en paramètre et exporte le fichier « cert » en '@mac'.pfx sur le serveur de certificat. Les paramètres du fichier cert sont définit dans le fichier '@mac'.inf, puis formatés en '@mac'.req. Le fichier de log garde le retour des commandes.

Les téléphones interrogeront le serveur pour récupérer le certificat qui correspondant à leur adresse MAC.

```
@echo off
if "%1"=="" goto nontrouve
if not exist "%1" goto nontrouve

rem Prend en params un fichier texte contenant une liste @mac (1/ligne)
rem Script qui génère un certificat '@mac'.crt en fonction de l'adresse mac passée en paramètre
rem Et qui exporte le cert en '@mac'.pfx
rem Les params du cert sont def dans le fichier '@mac'.inf, puis formatés en '@mac'.req
rem Le fichier de log garde le retour des commandes

mkdir .\inf
mkdir .\req
mkdir .\crt
mkdir .\log
for /F %%i in (%1) DO call :generation %%i
goto fin

:generation
        set logfile=log\log_%1.txt

        rem création du fichier .inf
        set inffile=inf\%1.inf

        rem params du fichier
        echo [Version] > "%inffile%"
        echo Signature="$Windows NT$" >> "%inffile%"

        echo [NewRequest]  >> "%inffile%"
        echo Subject = "CN=%1;OU=telephonie" >> "%inffile%"
                echo KeySpec = 1 >> "%inffile%"
        echo KeyLength = 1024 >> "%inffile%"
        echo Exportable = TRUE >> "%inffile%"
        echo MachineKeySet = FALSE >> "%inffile%"
        echo PrivateKeyArchive = FALSE  >> "%inffile%"
                echo UserProtected = FALSE >> "%inffile%"
                echo UseExistingKeySet = FALSE >> "%inffile%"
                echo RequestType = PKCS10 >> "%inffile%"
        echo KeyUsage = 0xa0 >> "%inffile%"

        echo [EnhancedKeyUsageExtension]  >> "%inffile%"
        rem echo OID=1.3.6.1.5.5.7.3.1 >> "%inffile%"
        echo OID=1.3.6.1.5.5.7.3.2 >> "%inffile%"

        echo [RequestAttributes]  >> "%inffile%"
        echo CertificateTemplate = ToIP >> "%inffile%"

        rem formatage de la requette
        rem echo ____Formatage de la requette : certreq.exe -new "inf\%1.inf" "req\%1.req"> "%logfile%"
        certreq.exe -new "inf\%1.inf" "req\%1.req" >> "%logfile%"

        rem verif de la requete (facultatif)
        rem echo ____Verif de la requete : certutil "req\%1.req" >> "%logfile%"
        rem certutil "req\%1.req" >> "%logfile%"

        rem creation du cert
        rem echo ____Creation du cert : certreq.exe -config srv01vas\svfca -submit "req\%1.req" "crt\%1.crt" >> "%logfile%"
        certreq.exe -config srv01vas\svfca -submit "req\%1.req" "crt\%1.crt" >> "%logfile%"

        rem validation
        rem echo ____Validation : certreq -accept "crt\%1.crt" >> "%logfile%"
        certreq -accept "crt\%1.crt" >> "%logfile%"

        rem export
        rem echo ____Export : certutil -f -v -p "" -user -exportpfx %1 "\\srv01vas\Certificat TOIP\%1.pfx" >> "%logfile%"
        certutil -f -v -p "" -user -exportpfx %1 "\\srv01vas\Certificat TOIP\%1.pfx" >> "%logfile%"

        rem suppr du cert du magasin de l'ordinateur
        rem echo ____SupprMag : certutil.exe -user -delstore my 0  >> "%logfile%"
        certutil.exe -user -delstore my 0 >> "%logfile%"

        rem suppr du fichier cert
        rem echo ____SupprFic : del crt\%1.crt >> "%logfile%"
        del crt\%1.crt

        rem suppr du fichier inf
        del inf\%1.inf

        rem suppr du fichier req
        del req\%1.req

        rem suppr du fichier log
        del log\log_%1.txt

        goto EOF

:nontrouve
        Fichier introuvable. Syntaxe : copysources.bat "nomfichier"

:fin
        rd /Q /S .\crt
        rd /Q /S .\inf
        rd /Q /S .\req
        rd /Q /S .\log
        cls

:EOF
```

Figure 55: Script de génération en masse des certificats téléphones.

Installation d'un certificat sur un téléphone

La procédure consiste à :

- Redémarrer le téléphone (débrancher le câble réseau),
- Lors de la phase d'initialisation du téléphone, avant que la phase 5 de l'initialisation commence, appuyer simultanément sur les touches i et #,
- Dans le menu principal, sélectionner Certificate,
- Sélectionner Get Certificate
- Dans le champ « Http », entrer l'adresse IP du serveur de certificat
- Modifier la valeur du champ Port
- Modifier le champ « Path » en tapant CertificatTOIP
- Cocher la case Use Mac@ File (le champ « File » se renseigne automatiquement par exemple 00809f904dcb.pfx)
- Appuyer sur la touche de validation pour enregistrer ces modifications

Le message « Fichier en cours d'obtention. Veuillez patienter... » s'affiche pendant que le terminal récupère le certificat.

Une fois le certificat téléchargé, le menu « Validation de l'obtention du certificat s'affiche ».

Il reste à valider pour que le terminal vérifie le certificat. Le nouveau certificat est affiché et stocké dans la mémoire flash en tant que nouveau certificat client.

Annexe 12
Configuration des commutateurs et des ACL

Configuration globale des commutateurs

La configuration globale de chaque pile de commutateur est modifiée avec les commandes suivantes :

- **aaa new-model**
- **aaa authentication dot1x default group radius** : envoie les requêtes d'authentification 802.1x vers les serveurs Radius,
- **aaa authorization network default group radius** : autorise le serveur RADIUS à assigner les VLAN aux ports des commutateurs,
- **dot1x system-auth-control** : active le 802.1x sur l'ensemble de la pile de commutateurs,
- **radius-server host 10.XX.XX.2 auth-port 1645 acct-port 1646 key clé_partagée**
- **radius-server host 10.XX.XX.3 auth-port 1645 acct-port 1646 key clé_partagée**

Ces deux dernières commandes définissent les serveurs Radius vers lesquels les requêtes doivent être envoyées.

Les deux commandes ci-dessous permettent l'outre passement de l'authentification 802.1x en cas d'indisponibilité des ACS :

- **dot1x critical eapol** : active le mode critique si les deux serveurs Radius ne sont pas joignables, ce qui permet d'autoriser le trafic sur le port. Le commutateur envoie un message EAPOL-Success et authentifie le port,
- **radius-server deadtime 5** : définit le temps en minutes pendant lequel le commutateur n'envoie plus de requêtes à un serveur RADIUS non joignable.

Configuration des ports des commutateurs

La configuration 802.1x sur les ports des commutateurs a été définie pour supporter les différents types d'authentification 802.1x validés (MAB, EAP-TLS, PEAP). Ainsi quelque soit le type d'équipement connecté dans le futur, aucune modification ne sera à faire sur les ports.

- **dot1x pae authenticator** : active l'authentification 802.1X via EAP,
- **authentication port-control auto** : active le 802.1x en mode automatique et permet au commutateur de répondre aux requêtes EAP des supplicants,
- **authentication host-mode multi-domain** : active le mode multi domaine qui permet sur un seul port de connecter un équipement data et un équipement voix,
- **authentication control-direction in**
- **authentication periodic**
- **authentication timer reauthenticate server** : active la réauthentification 802.1x et permet au serveur ACS d'envoyer la durée de la session,
- **authentication violation restrict** : bloque la nouvelle authentification en cas de violation au lieu de la fermeture du port du commutateur. Cette fonctionnalité nous permet de ne pas bloquer l'ordinateur si le téléphone sur lequel il est raccordé n'a pas de certificat,
- **dot1x timeout tx-period 10** : il s'agit du temps d'attente entre les deux requêtes EAP Identity request envoyées par le commutateur (par défaut 30 secondes), l'intérêt de le diminuer est de diminuer le temps d'authentification,
- **authentication event fail action authorize vlan 999** : définit le vlan à appliquer dans le cas d'un échec d'authentification,
- **authentication event no-response action authorize vlan 999** : définit le vlan à appliquer dans le cas d'une non réponse pendant la phase d'authentification,
- **Mab** : active le Mac Authentication Bypass pour permettre aux équipements non compatibles 802.1x d'être authentifiés par leur adresse MAC.

Les deux commandes ci-dessous permettent l'outre passement de l'authentification 802.1x en cas d'indisponibilité des serveurs ACS :

- **authentication event server dead action authorize**
- **authentication event server alive action reinitialize**

Configuration des ACL sur le cœur de réseau

Tout d'abord il s'agit de créer la liste des flux qui seront autorisés :

Figure 56: ACL GUEST.

Ensuite on applique cette ACL sur l'interface du VLAN 300 :

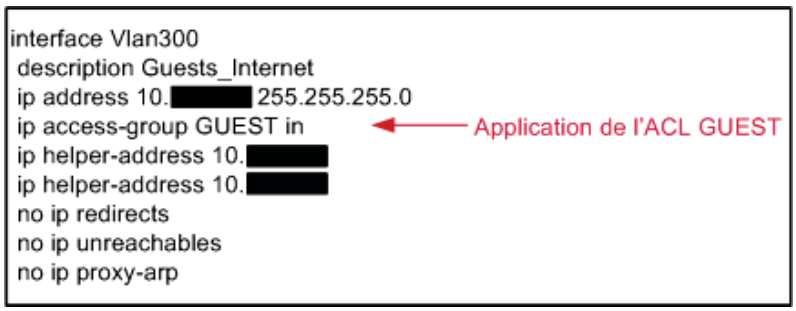


Figure 57: Application de l'ACL GUEST.

Annexe 13
Configuration des serveurs ACS

Comme nous utilisons deux boitiers ACS, il y a un primaire et un secondaire et toutes les modifications de configuration sur l'ACS sont faites sur l'ACS primaire à partir d'une interface web.

On y définit :

- Les commutateurs et la clé partagée pour qu'il communique les trames d'authentification,
- On ajoute également toutes les adresses MAC des équipements (imprimantes, badgeuse, contrôle d'accès, …) pour qu'ils soient authentifiés.

Ajout des systèmes authentificateurs dans l'ACS

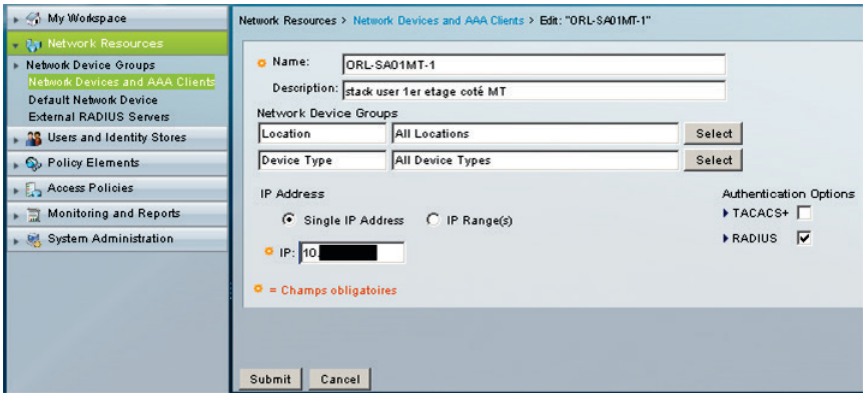


Figure 58: Ajout d'un système authentificateur.

Configuration des groupes d'identité

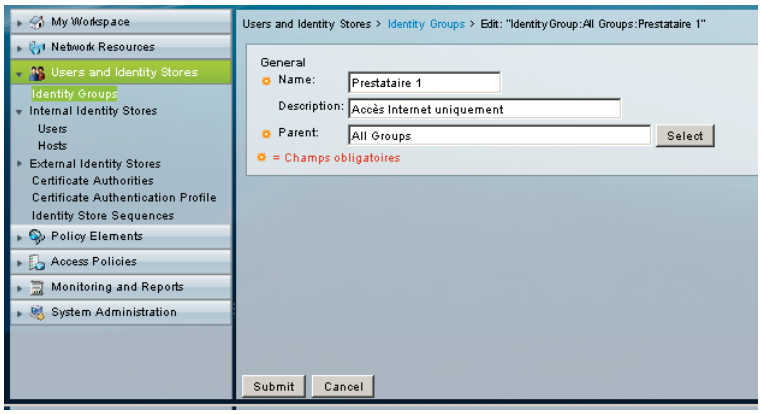


Figure 59: Ajout d'un groupe.

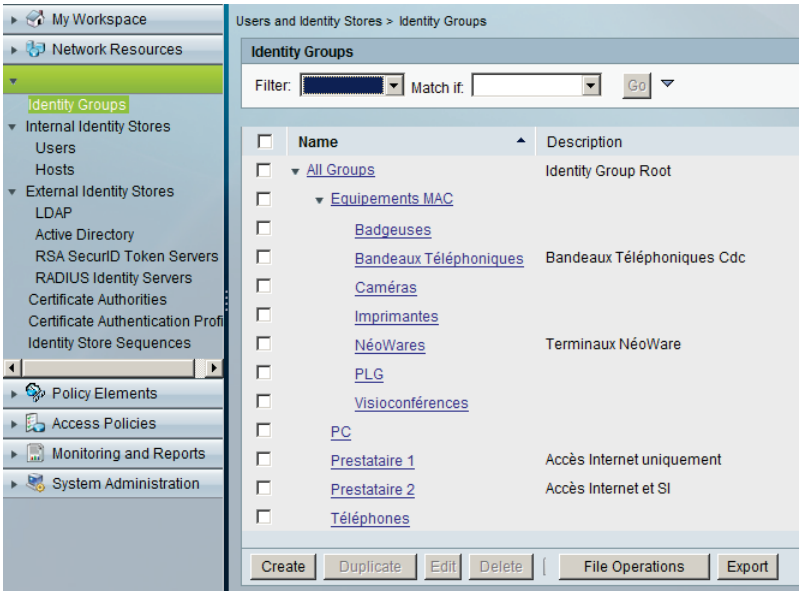


Figure 60: Inventaire des groupes créés.

Configuration des utilisateurs

Les comptes utilisateurs peuvent être utilisés pour la connexion aux équipements (Switch) via une authentification Radius mais également dans le processus d'authentification 802.1x (PEAP..). Des règles doivent être créées afin de spécifier quelles autorisations d'accès sont attribuées aux comptes créés.

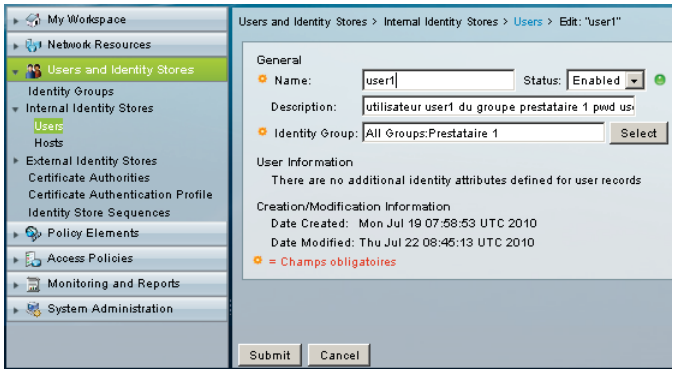


Figure 61: Création d'un utilisateur.

Configuration des hôtes

Les hôtes dans cette section correspondent aux équipements authentifiés par la méthode MAB (Mac Adress Bypass).

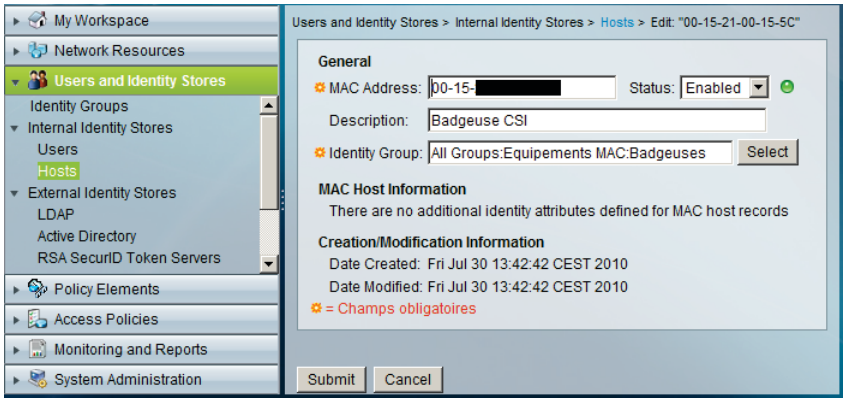


Figure 62: Ajout d'un hôte.

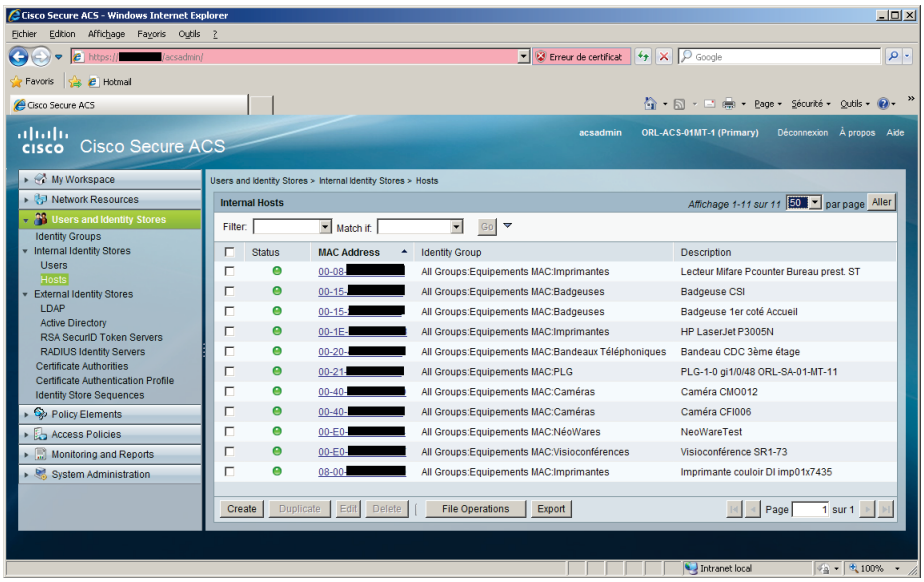


Figure 63: Exemple d'hôtes enregistrés.

Création de la liaison avec l'Active Directory

Cette section permet de renseigner une base de compte externe à l'ACS. Elle garantit la communication entre l'ACS et l'Active Directory. Elle est par exemple utilisée pour l'authentification des machines utilisant un certificat et le sera pour autoriser les comptes créés dans l'AD pour être authentifiés.

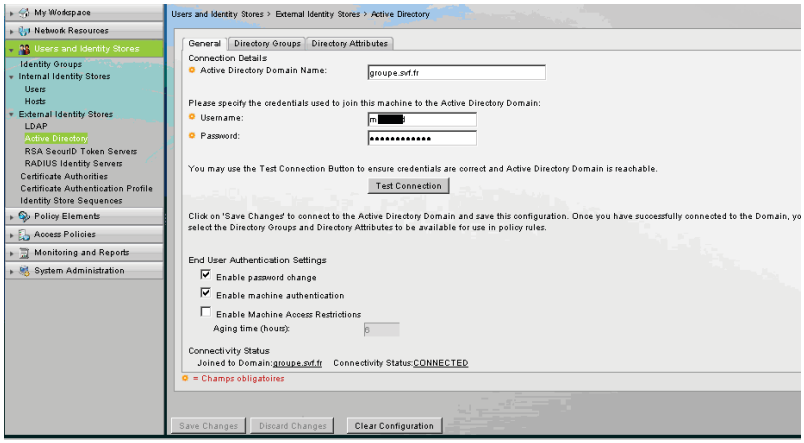


Figure 64: Création de la liaison avec l'Active Directory.

Création de la liaison avec l'autorité de certification

Déclaration de l'autorité de certification SVF dans L'ACS.

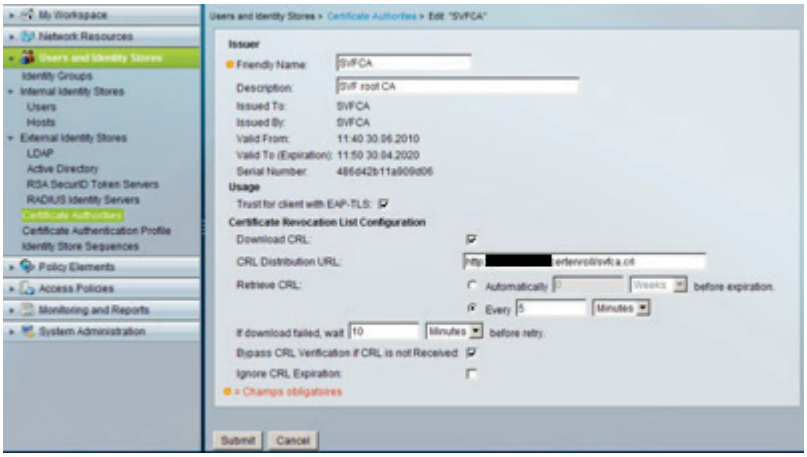


Figure 65: Création de la liaison avec l'autorité de certification.

Le paramètre « Bypass CRL » permet de passer outre le blocage de tous les utilisateurs authentifiés en cas d'indisponibilité du serveur.

Configuration du profil d'authentification par certificat

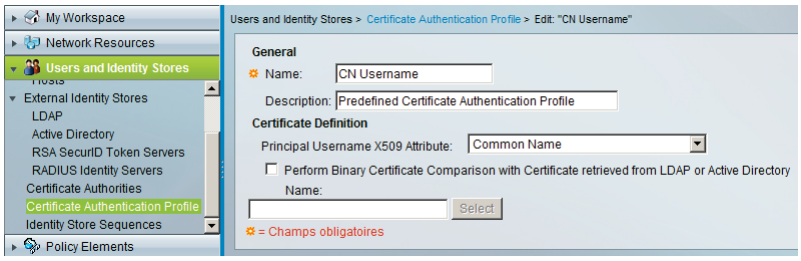


Figure 66: Création du profil d'authentification par certificat.

Configuration des Identity Sequences

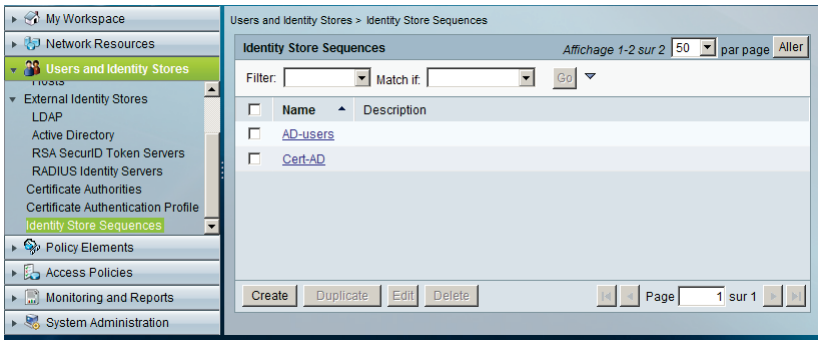


Figure 67: Liste des séquences d'identification.

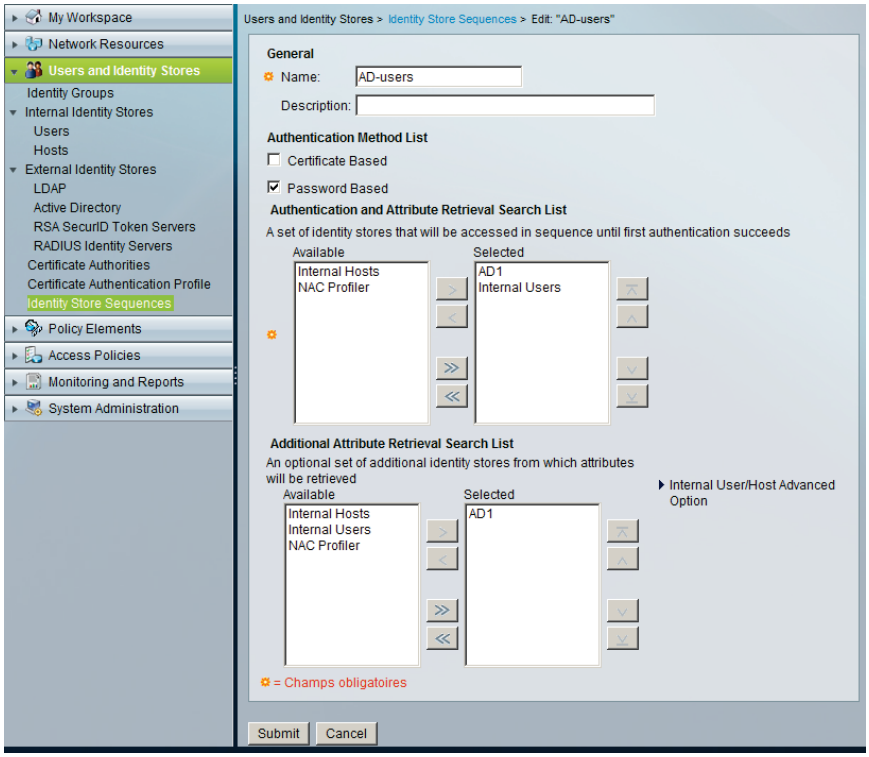


Figure 68: Séquence d'identification pour les comptes AD.

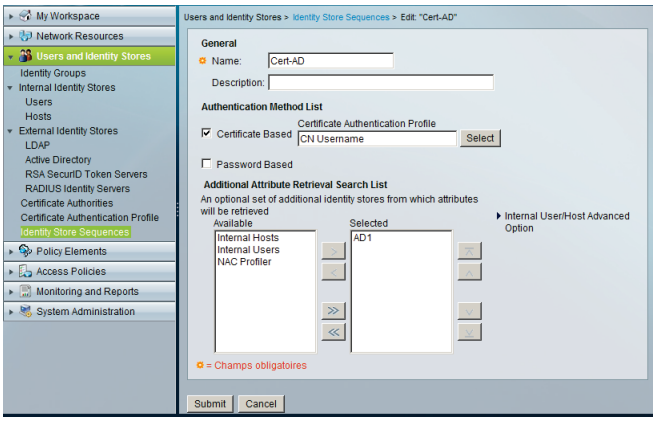


Figure 69: Séquence d'identification pour les certificats.

Configuration des profils d'autorisation

Paramétrage pour les ordinateurs et les équipements authentifiés par adresse MAC:

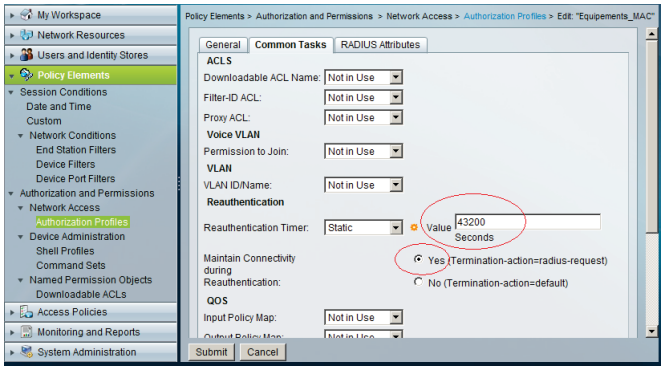


Figure 70: Configuration du profil d'autorisation pour les ordinateurs et les équipements authentifiés par adresse MAC.

Paramétrage pour les téléphones :

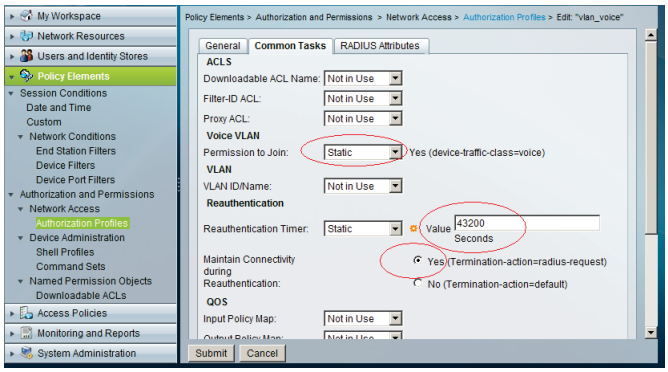


Figure 71: Configuration du profil d'autorisation pour les téléphones.

Configuration de l'accès par défaut autorisé

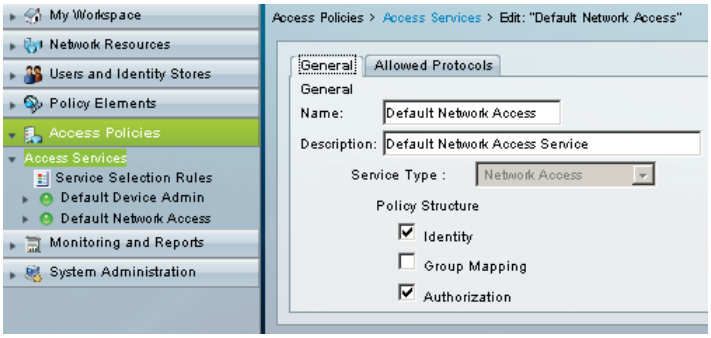


Figure 72: Configuration de l'accès par défaut.

Configuration des protocoles autorisés

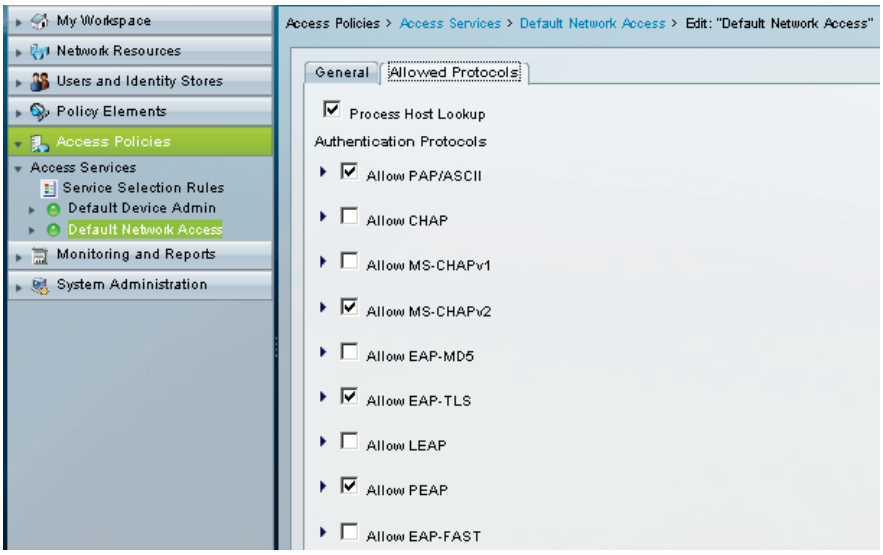


Figure 73: Choix des protocoles autorisés.

Configuration des règles pour les services

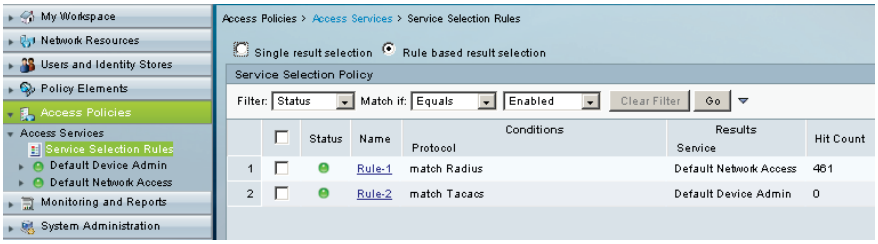


Figure 74: Règles par service.

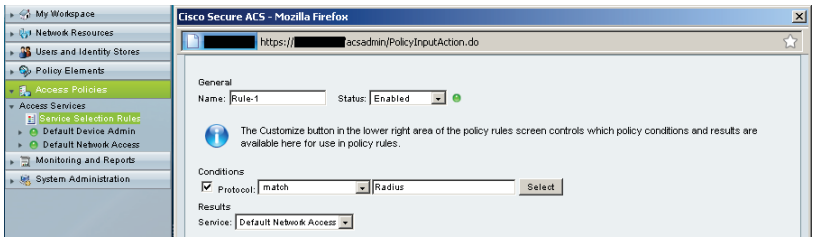


Figure 75: Configuration des règles RADIUS.

Configuration des règles d'identification

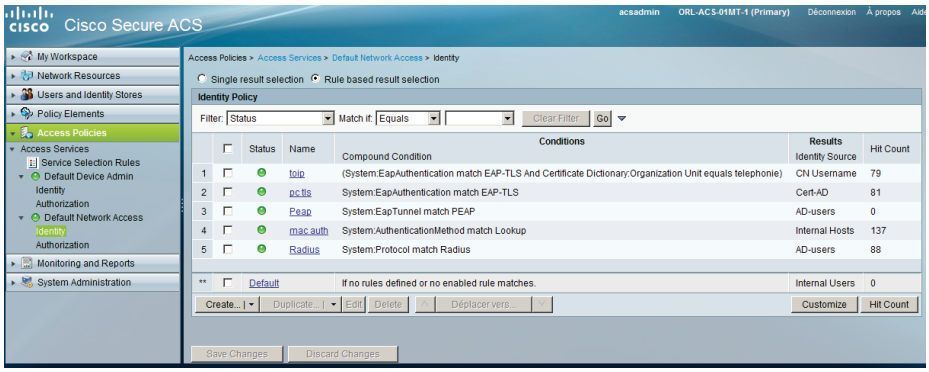


Figure 76: Règles d'identification.

Configuration des règles d'accès autorisation

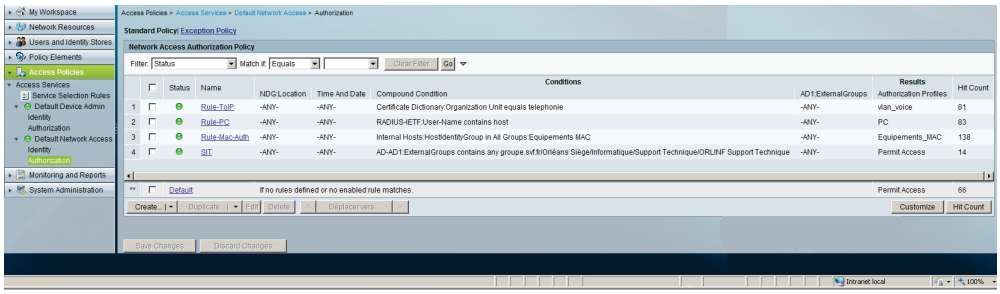


Figure 77: Règles d'autorisation.

Configuration des rapports d'alertes

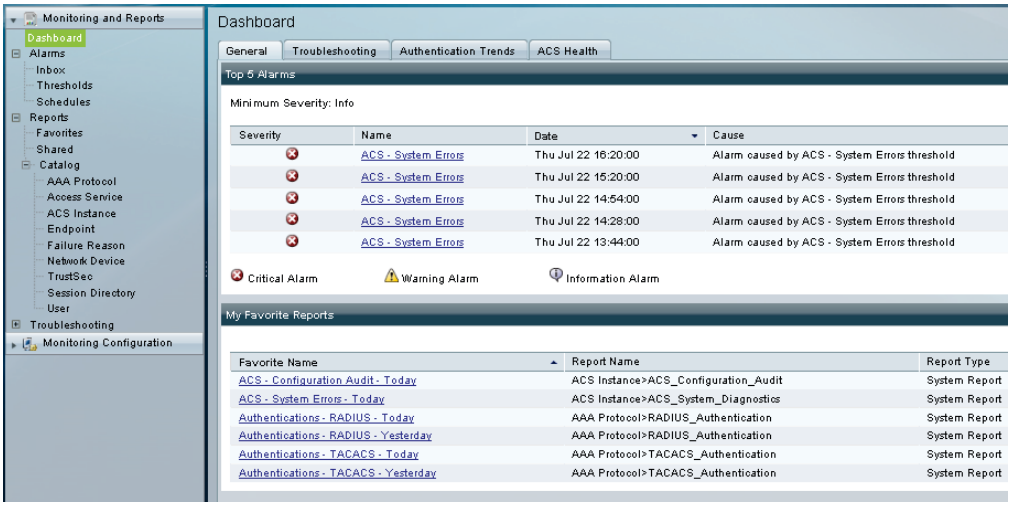


Figure 78: Rapports d'alertes RADIUS.

Annexe 14
Configuration du serveur d'annuaire

Création du groupe pour les ordinateurs SVF :

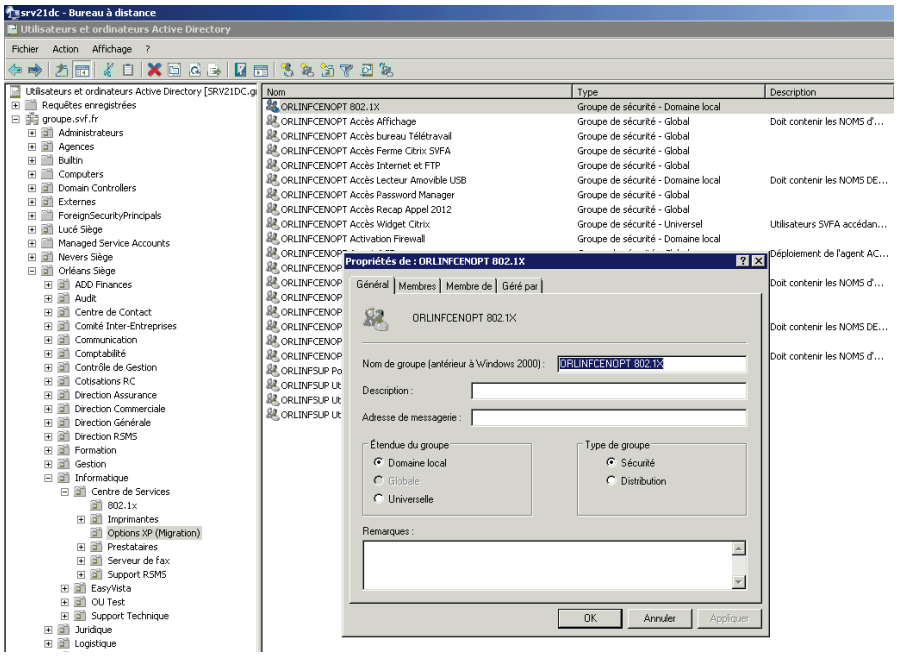


Figure 79: Groupe de sécurité pour les ordinateurs SVF.

Création du groupe pour l'accès des prestataires :

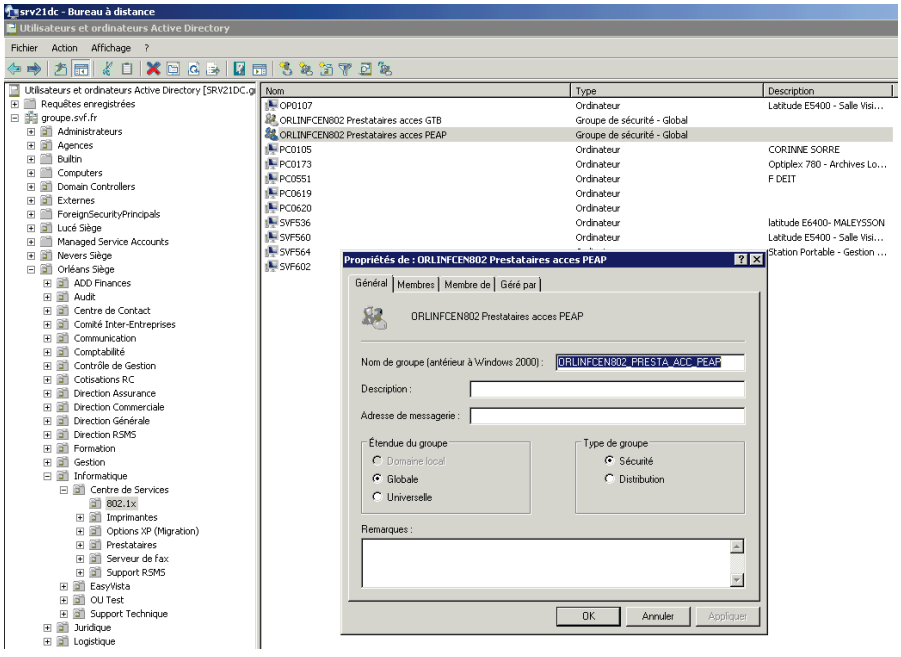


Figure 80: Groupe de sécurité pour les prestataires internet.

Annexe 15
Configuration des GPO

Création de la stratégie de configuration automatique des cartes réseaux :

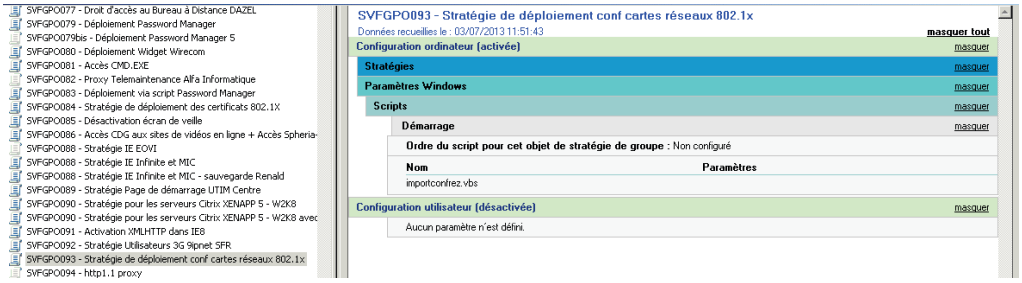


Figure 81: Stratégie pour la configuration automatique des cartes réseaux des ordinateurs.

Création de la stratégie pour le déploiement et la mise à jour des certificats ordinateurs :

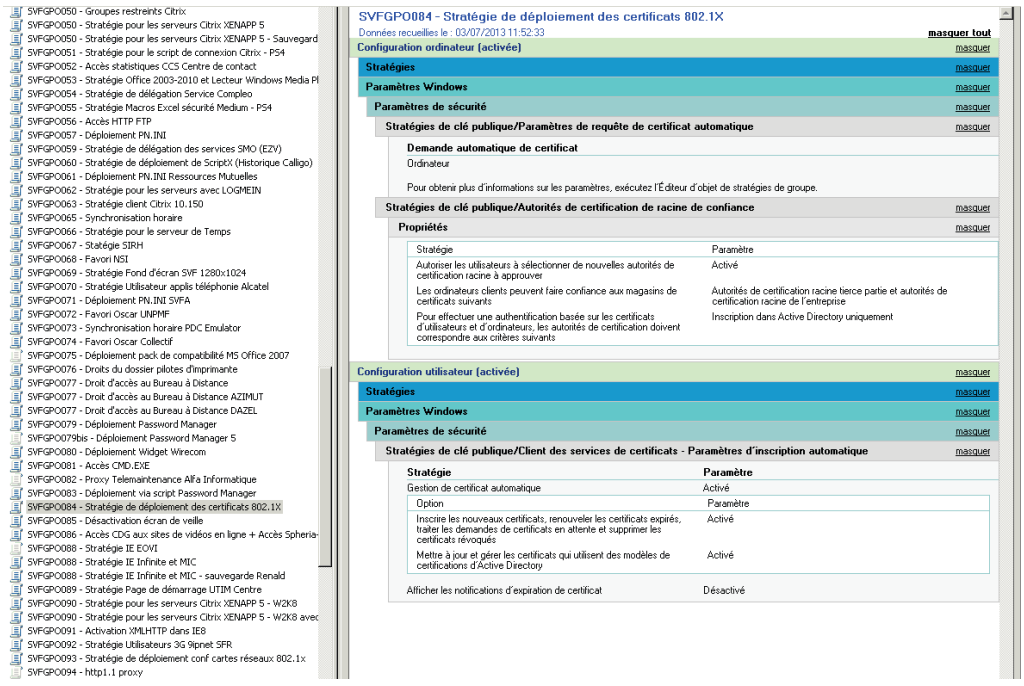
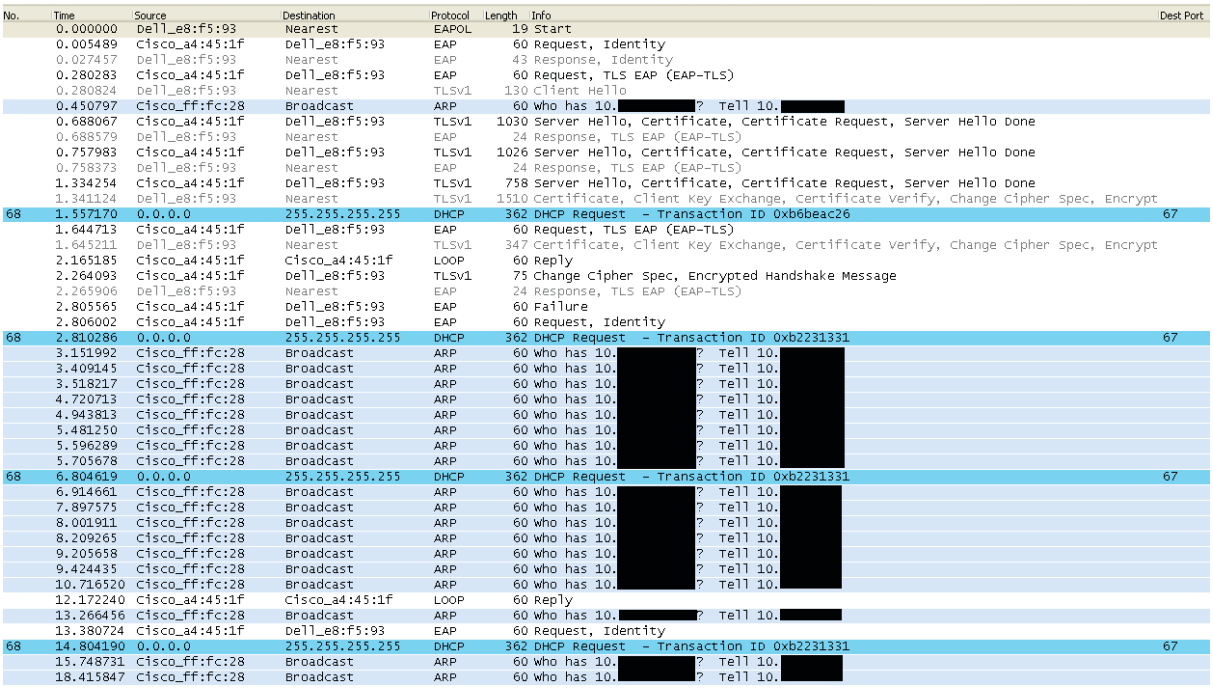


Figure 82: Stratégie de déploiement des certificats ordinateurs.

Annexe 16
Exemple d'échanges lors d'une authentification 802.1x pour un ordinateur SVF



No.	Time	Source	Destination	Protocol	Length	Info	Dest Port
	0.000000	Dell_e8:f5:93	Nearest	EAPOL	19	Start	
	0.005489	Cisco_a4:45:1f	Dell_e8:f5:93	EAP	60	Request, Identity	
	0.027457	Dell_e8:f5:93	Nearest	EAP	43	Response, Identity	
	0.280283	Cisco_a4:45:1f	Dell_e8:f5:93	EAP	60	Request, TLS EAP (EAP-TLS)	
	0.280824	Dell_e8:f5:93	Nearest	TLSv1	130	Client Hello	
	0.450797	Cisco_ff:fc:28	Broadcast	ARP	60	Who has 10.[redacted]? Tell 10.[redacted]	
	0.688067	Cisco_a4:45:1f	Dell_e8:f5:93	TLSv1	1030	Server Hello, Certificate, Certificate Request, Server Hello Done	
	0.688579	Dell_e8:f5:93	Nearest	EAP	24	Response, TLS EAP (EAP-TLS)	
	0.757983	Cisco_a4:45:1f	Dell_e8:f5:93	TLSv1	1026	Server Hello, Certificate, Certificate Request, Server Hello Done	
	0.758373	Dell_e8:f5:93	Nearest	EAP	24	Response, TLS EAP (EAP-TLS)	
	1.334254	Cisco_a4:45:1f	Dell_e8:f5:93	TLSv1	758	Server Hello, Certificate, Certificate Request, Server Hello Done	
	1.341124	Dell_e8:f5:93	Nearest	TLSv1	1510	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypt	
68	1.557170	0.0.0.0	255.255.255.255	DHCP	362	DHCP Request - Transaction ID 0xb6beac26	67
	1.644713	Cisco_a4:45:1f	Dell_e8:f5:93	EAP	60	Request, TLS EAP (EAP-TLS)	
	1.645211	Dell_e8:f5:93	Nearest	TLSv1	347	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypt	
	2.165185	Cisco_a4:45:1f	Cisco_a4:45:1f	LOOP	60	Reply	
	2.264093	Cisco_a4:45:1f	Dell_e8:f5:93	TLSv1	75	Change Cipher Spec, Encrypted Handshake Message	
	2.265906	Dell_e8:f5:93	Nearest	EAP	24	Response, TLS EAP (EAP-TLS)	
	2.805565	Cisco_a4:45:1f	Dell_e8:f5:93	EAP	60	Failure	
	2.806002	Cisco_a4:45:1f	Dell_e8:f5:93	EAP	60	Request, Identity	
68	2.810286	0.0.0.0	255.255.255.255	DHCP	362	DHCP Request - Transaction ID 0xb2231331	67
	3.151992	Cisco_ff:fc:28	Broadcast	ARP	60	Who has 10.[redacted]? Tell 10.[redacted]	
	3.409145	Cisco_ff:fc:28	Broadcast	ARP	60	Who has 10.[redacted]? Tell 10.[redacted]	
	3.518217	Cisco_ff:fc:28	Broadcast	ARP	60	Who has 10.[redacted]? Tell 10.[redacted]	
	4.720713	Cisco_ff:fc:28	Broadcast	ARP	60	Who has 10.[redacted]? Tell 10.[redacted]	
	4.943813	Cisco_ff:fc:28	Broadcast	ARP	60	Who has 10.[redacted]? Tell 10.[redacted]	
	5.481250	Cisco_ff:fc:28	Broadcast	ARP	60	Who has 10.[redacted]? Tell 10.[redacted]	
	5.596289	Cisco_ff:fc:28	Broadcast	ARP	60	Who has 10.[redacted]? Tell 10.[redacted]	
	5.705678	Cisco_ff:fc:28	Broadcast	ARP	60	Who has 10.[redacted]? Tell 10.[redacted]	
68	6.804619	0.0.0.0	255.255.255.255	DHCP	362	DHCP Request - Transaction ID 0xb2231331	67
	6.914661	Cisco_ff:fc:28	Broadcast	ARP	60	Who has 10.[redacted]? Tell 10.[redacted]	
	7.897575	Cisco_ff:fc:28	Broadcast	ARP	60	Who has 10.[redacted]? Tell 10.[redacted]	
	8.001911	Cisco_ff:fc:28	Broadcast	ARP	60	Who has 10.[redacted]? Tell 10.[redacted]	
	8.209265	Cisco_ff:fc:28	Broadcast	ARP	60	Who has 10.[redacted]? Tell 10.[redacted]	
	9.205658	Cisco_ff:fc:28	Broadcast	ARP	60	Who has 10.[redacted]? Tell 10.[redacted]	
	9.424435	Cisco_ff:fc:28	Broadcast	ARP	60	Who has 10.[redacted]? Tell 10.[redacted]	
	10.716520	Cisco_ff:fc:28	Broadcast	ARP	60	Who has 10.[redacted]? Tell 10.[redacted]	
	12.172240	Cisco_a4:45:1f	Cisco_a4:45:1f	LOOP	60	Reply	
	13.266456	Cisco_ff:fc:28	Broadcast	ARP	60	Who has 10.[redacted]? Tell 10.[redacted]	
	13.380724	Cisco_a4:45:1f	Dell_e8:f5:93	EAP	60	Request, Identity	
68	14.804190	0.0.0.0	255.255.255.255	DHCP	362	DHCP Request - Transaction ID 0xb2231331	67
	15.748731	Cisco_ff:fc:28	Broadcast	ARP	60	Who has 10.[redacted]? Tell 10.[redacted]	
	18.415847	Cisco_ff:fc:28	Broadcast	ARP	60	Who has 10.[redacted]? Tell 10.[redacted]	

Figure 83: Capture de trafic lors d'une authentification 802.1x.

Annexe 17
Processus de traitement des requêtes 802.1x par le serveur ACS

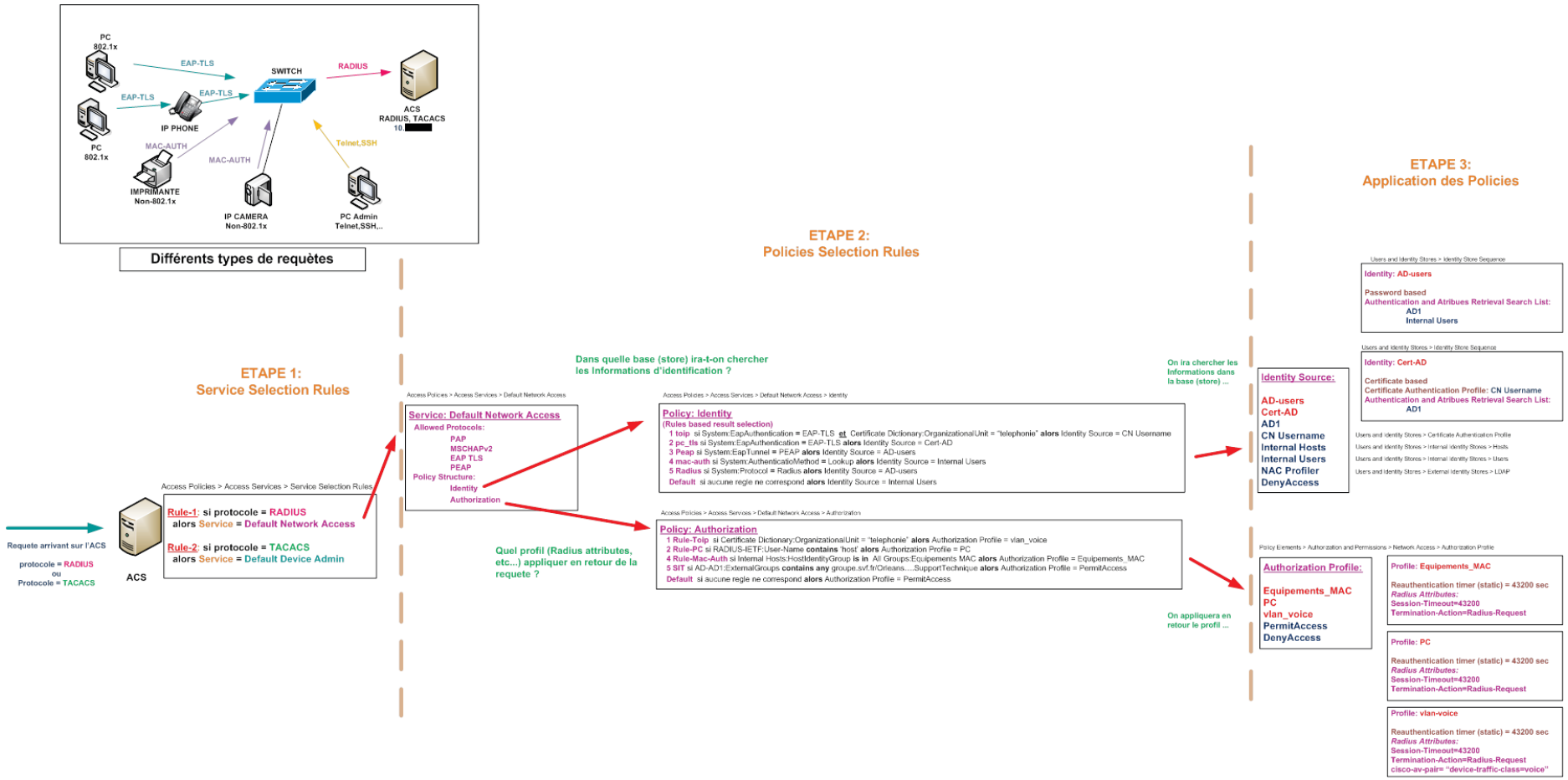


Figure 84: Processus de traitement des requêtes 802.1x par le serveur ACS.

Annexe 18
Procédures de déploiement des nouveaux matériels

Les procédures ci-dessous représentent schématiquement les étapes à respecter lors de l'installation d'un nouvel équipement.

Elles sont intégrées de façon plus détaillée aux modes opératoires utilisés par les techniciens en charge du déploiement de matériel.

Procédure d'installation d'un nouvel ordinateur SVF

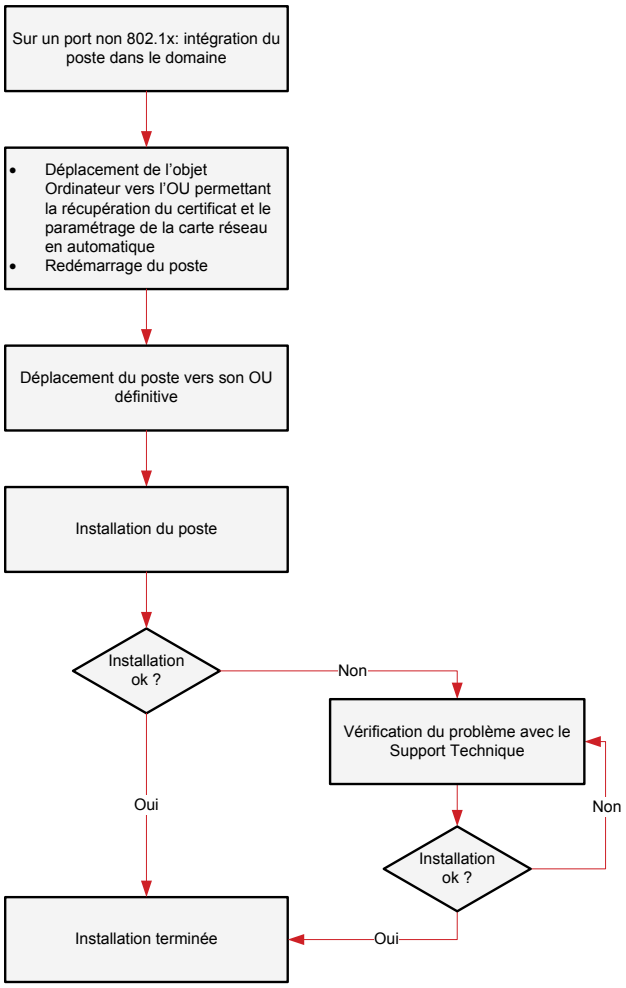


Figure 85: Procédure d'installation d'un nouvel ordinateur SVF.

Procédure d'installation d'un nouveau téléphone SVF

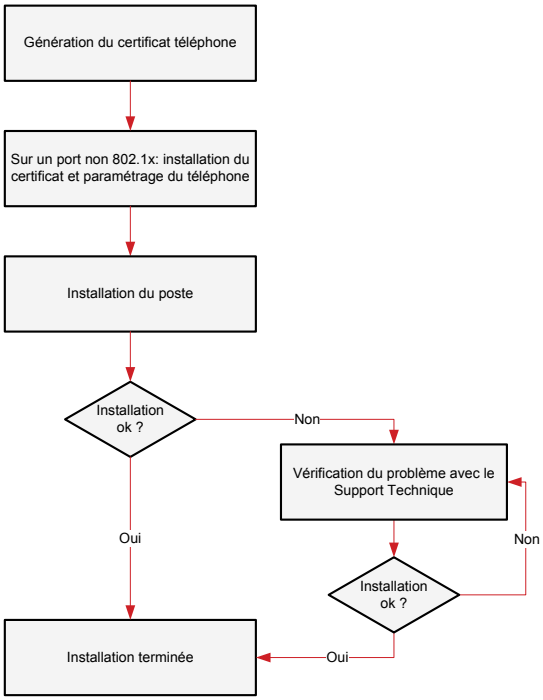


Figure 86: Procédure d'installation d'un nouveau téléphone SVF.

Procédure d'installation d'un nouvel équipement non 802.1x

Pour l'installation d'un matériel non 802.1x il suffit de relever l'adresse MAC de celui-ci pour le déclarer au niveau du serveur Radius.

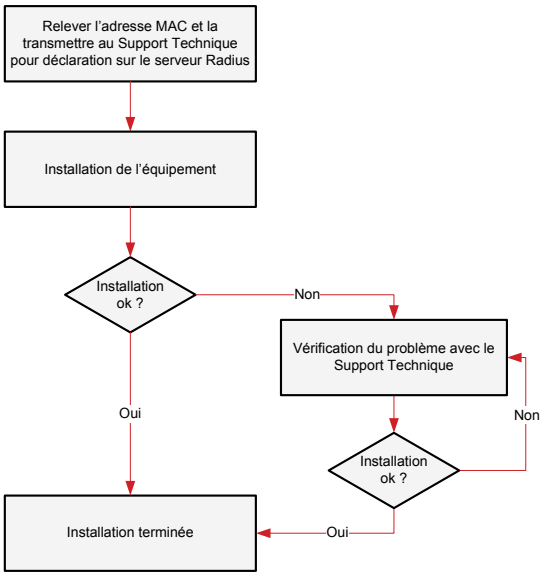


Figure 87: Procédure d'installation d'un équipement non 802.1x.

Références

Bibliographie

BORDERES S., 2007. Authentification réseau avec RADIUS. Editions Eyrolles, 225 p.

BROWN E. L., 2007. Port-based authentication. Auerbach Publications, 254 p.

GEIER J., 2008. Implementing 802.1x security solutions for wired and wireless networks. Wiley Publishing, 356 p.

GUIDARINI S., DESSE S., 2005. Etat de l'art de la sécurité informatique

MISHRA A., ARBAUGH W., 2002. An initial security analysis of the IEEE 802.1x standard. Department of computer science, University of Maryland, [en ligne]. Disponible sur : http://www.cs.umd.edu/~waa/1x.pdf. (consulté le 6 juin 2011).

SACCAVINI L., 2003. Le protocole IEEE 802.1x. INRIA, [en ligne]. Disponible sur https://aresu.dsi.cnrs.fr/IMG/pdf/secu.CNRS.vCARS2003.saccavini.pdf. (consulté le 6 juin 2011).

SACCAVINI L., 2003. 802.1x et la sécurisation de l'accès au réseau local. INRIA, [en ligne]. Disponible sur http://2003.jres.org/actes/paper.111.pdf. (consulté le 6 juin 2011).

SAILLARD C., 2003. 802.1x : Solution d'authentification sécurisée pour le futur réseau sans fil de l'Université Louis Pasteur. Université Louis Pasteur, [en ligne]. Disponible sur http://2003.jres.org/actes/paper.143.pdf. (consulté le 9 juin 2011).

YOUNUS M., 2000-2005. Wired 802.1x Security. SANS Institute, [en ligne]. Disponible sur http://www.sans.org/reading_room/whitepapers/firewalls/wired-8021x-security_1654. (consulté le 9 juin 2011).

SIX N., 2002. Le danger vient de l'intérieur de la citadelle informatique. JDNet, [en ligne]. Disponible sur http://www.journaldunet.com/solutions/0210/021002_secu.shtml. (consulté le 6 février 2012).

PILLOU J.F. Méthodologie d'une intrusion sur un réseau. CommentCaMarche.net, [en ligne]. Disponible sur http://nocremetz.free.fr/ccm/attaques/methodologie.htm. (consulté le 6 février 2012).

DOREAU E., 2007. *Sécurisation d'une architecture réseau dans un centre hospitalier*. Mémoire d'ingénieur, CNAM de Montpellier, 140 pages, [en ligne]. Disponible sur http://emmanueldoreau.free.fr/backup/CNAM/MEMOIRE. (consulté le 9 juin 2011).

TOUCAS-TRUYEN P., 2011. Les mutuelles à un tournant – Les corps intermédiaires en perspective. Constructif, FFB [en ligne]. Disponible sur http://www.constructif.fr/bibliotheque/2011-11/les-mutuelles-a-un-tournant.html?item_id=3123. (consulté le 20 avril 2012).

Sites web

http://www.cisco.com
Site du constructeur Cisco.
http://www.ietf.org
Site de l'IETF.
http://www.ieee.org
Site de l'IEEE.
http://www.microsoft.com
Site de Microsoft.
http://www.wikipedia.org
Encyclopédie libre.
http://www.alcatel.com
Site de Alcatel-Lucent.

Liste des figures

FIGURE 1: PRESENTATION DE SPHERIA VAL DE FRANCE. 13
FIGURE 2: ORGANIGRAMME DU DEPARTEMENT INFORMATIQUE 15
FIGURE 3: LE RESEAU GLOBAL DE SVF. 18
FIGURE 4: TECHNOLOGIE CISCO VIRTUAL SWITCHING SYSTEM. 19
FIGURE 5: ARCHITECTURE RESEAU DU SIEGE SOCIAL DE SVF. 20
FIGURE 6: PROCESSUS D'AUTHENTIFICATION. 21
FIGURE 7: PARE-FEU DE PERIMETRE. 22
FIGURE 8: PERIMETRE EN 3 PARTIES. 23
FIGURE 9: PARE-FEUX DOS A DOS. 23
FIGURE 10: METHODOLOGIE GLOBALE D'INTRUSION. 26
FIGURE 11: PLANNING DU PROJET. 30
FIGURE 12: ARCHITECTURE RESEAU DU SITE ORLEANS JAURES. 32
FIGURE 13: LES 3 ENTITES QUI INTERAGISSENT DANS LE PROTOCOLE 802.1X. 33
FIGURE 14: ÉTAT DU PAE AVANT LA PHASE D'AUTHENTIFICATION. 34
FIGURE 15: ÉTAT DU PAE APRES UNE AUTHENTIFICATION REUSSIE. 34
FIGURE 16: LES DIFFERENTS PROTOCOLES COMPOSANT LE 802.1X. 35
FIGURE 17: EXEMPLE DE DIALOGUE LORS DU PROCESSUS D'AUTHENTIFICATION. 36
FIGURE 18: EXEMPLE DE DIALOGUE LORSQUE LE SUPPLICANT N'EST PAS CONFIGURE. 36
FIGURE 19: EXEMPLE DE DIALOGUE SANS AUTHENTIFICATEUR, SUPPLICANT EN MODE PASSIF. 37
FIGURE 20: EXEMPLE DE DIALOGUE SANS AUTHENTIFICATEUR, SUPPLICANT EN MODE ACTIF. 37
FIGURE 21: EXEMPLE DE DIALOGUE SANS SERVEUR D'AUTHENTIFICATION. 38
FIGURE 22: ENCAPSULATION DES TRAMES EAP. 38
FIGURE 23: FORMAT DU PAQUET EAP. 39
FIGURE 24: EXEMPLE D'UN DIALOGUE EAP. 40
FIGURE 25: LES DIFFERENTES COUCHES DU PROTOCOLE EAP. 41
FIGURE 26: FORMAT DU PAQUET EAPOL. 42
FIGURE 27: FORMAT DU PAQUET EAP-METHOD. 43
FIGURE 28: PRINCIPE DE L'AUTHENTIFICATION RADIUS-MAC. 52
FIGURE 29: PRINCIPE DE L'AUTHENTIFICATION 802.1X. 53
FIGURE 30: FORMAT DU PAQUET RADIUS. 54
FIGURE 31: FORMAT DU CHAMP ATTRIBUTS ET VALEURS. 56
FIGURE 32: LES COMPOSANTS DE L'ARCHITECTURE 802.1X CHEZ SVF. 57
FIGURE 33: METHODES D'AUTHENTIFICATION EAP. 62
FIGURE 34: AFFECTATION DES VLAN. 69
FIGURE 35: MAQUETTE 802.1X. 70
FIGURE 36: TRAMES UTILISEES POUR LES CERTIFICATS. 73
FIGURE 37: EXEMPLE DE REQUETE DE CERTIFICAT POUR UN TELEPHONE. 73
FIGURE 38: NOUVELLES REGLES IDENTITY. 78
FIGURE 39: NOUVELLES REGLES AUTHORIZATION. 78

FIGURE 40: PROCEDURE DE MIGRATION DES EQUIPEMENTS. 81
FIGURE 41: PROCESSUS D'AUTHENTIFICATION. 91
FIGURE 42: ACTIVATION DE L'AUTHENTIFICATION ET CHOIX DE LA METHODE. 98
FIGURE 43: SELECTION DU CERTIFICAT. 98
FIGURE 44: COMMANDE D'EXPORT DE LA CONFIGURATION DE LA CARTE RESEAU. 99
FIGURE 45: FICHIER DE CONFIGURATION DE LA CARTE RESEAU. 99
FIGURE 46: COMMANDE D'IMPORT DE LA CONFIGURATION DE LA CARTE RESEAU. 99
FIGURE 47: GROUPE POUR LES ORDINATEURS 802.1X. 100
FIGURE 48: VERIFICATION DE LA PRESENCE DU CERTIFICAT. 100
FIGURE 49: ACTIVATION DE L'AUTHENTIFICATION SUR UN ORDINATEUR PRESTATAIRE. 101
FIGURE 50: CHOIX DE LA METHODE D'AUTHENTIFICATION. 102
FIGURE 51: LA CONNEXION RESEAU NECESSITE UNE IDENTIFICATION. 102
FIGURE 52: SAISIE DES INFORMATIONS D'IDENTIFICATION. 102
FIGURE 53: SCRIPT DE CONFIGURATION DE LA CARTE RESEAU. 103
FIGURE 54: LOGIGRAMME DU PROGRAMME DE GENERATION DES CERTIFICATS TELEPHONES. 104
FIGURE 55: SCRIPT DE GENERATION EN MASSE DES CERTIFICATS TELEPHONES. 105
FIGURE 56: ACL GUEST 109
FIGURE 57: APPLICATION DE L'ACL GUEST. 109
FIGURE 58: AJOUT D'UN SYSTEME AUTHENTIFICATEUR. 110
FIGURE 59: AJOUT D'UN GROUPE. 111
FIGURE 60: INVENTAIRE DES GROUPES CREES. 111
FIGURE 61: CREATION D'UN UTILISATEUR. 112
FIGURE 62: AJOUT D'UN HOTE. 112
FIGURE 63: EXEMPLE D'HOTES ENREGISTRES. 113
FIGURE 64: CREATION DE LA LIAISON AVEC L'ACTIVE DIRECTORY. 113
FIGURE 65: CREATION DE LA LIAISON AVEC L'AUTORITE DE CERTIFICATION. 114
FIGURE 66: CREATION DU PROFIL D'AUTHENTIFICATION PAR CERTIFICAT. 114
FIGURE 67: LISTE DES SEQUENCES D'IDENTIFICATION. 115
FIGURE 68: SEQUENCE D'IDENTIFICATION POUR LES COMPTES AD. 115
FIGURE 69: SEQUENCE D'IDENTIFICATION POUR LES CERTIFICATS. 116
FIGURE 70: CONFIGURATION DU PROFIL D'AUTORISATION POUR LES ORDINATEURS ET LES EQUIPEMENTS AUTHENTIFIES PAR ADRESSE MAC. 116
FIGURE 71: CONFIGURATION DU PROFIL D'AUTORISATION POUR LES TELEPHONES. 116
FIGURE 72: CONFIGURATION DE L'ACCES PAR DEFAUT. 117
FIGURE 73: CHOIX DES PROTOCOLES AUTORISES. 117
FIGURE 74: REGLES PAR SERVICE. 117
FIGURE 75: CONFIGURATION DES REGLES RADIUS. 118
FIGURE 76: REGLES D'IDENTIFICATION. 118
FIGURE 77: REGLES D'AUTORISATION. 118
FIGURE 78: RAPPORTS D'ALERTES RADIUS. 119

FIGURE 79: GROUPE DE SECURITE POUR LES ORDINATEURS SVF..... 120
FIGURE 80: GROUPE DE SECURITE POUR LES PRESTATAIRES INTERNET. 120
FIGURE 81: STRATEGIE POUR LA CONFIGURATION AUTOMATIQUE DES CARTES RESEAUX DES ORDINATEURS..... 121
FIGURE 82: STRATEGIE DE DEPLOIEMENT DES CERTIFICATS ORDINATEURS. 121
FIGURE 83: CAPTURE DE TRAFIC LORS D'UNE AUTHENTIFICATION 802.1X. 122
FIGURE 84: PROCESSUS DE TRAITEMENT DES REQUETES 802.1X PAR LE SERVEUR ACS. 123
FIGURE 85: PROCEDURE D'INSTALLATION D'UN NOUVEL ORDINATEUR SVF..... 124
FIGURE 86: PROCEDURE D'INSTALLATION D'UN NOUVEAU TELEPHONE SVF..... 125
FIGURE 87: PROCEDURE D'INSTALLATION D'UN EQUIPEMENT NON 802.1X. 125

Liste des tableaux

TABLEAU I : COMPARATIF DES ARCHITECTURES DE FIREWALL 24
TABLEAU II: TYPES DE PAQUETS EAP. 39
TABLEAU III: LISTE DES SYSTEMES SVF A AUTHENTIFIER. 57
TABLEAU IV: COMPARATIF DES CONTRAINTES POUR UN ORDINATEUR PRESTATAIRE. 60
TABLEAU V: COMPARATIF DES CONTRAINTES POUR UN ORDINATEUR DE PRET SVF. 61
TABLEAU VI: METHODES EAP SUPPORTEES PAR SYSTEME. 63
TABLEAU VII: METHODES EAP SUPPORTEES PAR CISCO ACS. 63
TABLEAU VIII: METHODES EAP SUPPORTEES PAR MICROSOFT ACTIVE DIRECTORY. 64
TABLEAU IX: RECAPITULATIF DES METHODES SUPPORTEES PAR SYSTEME. 64
TABLEAU X: METHODES RETENUES PAR SYSTEME. 67
TABLEAU XI: VLAN EN PRODUCTION. 68
TABLEAU XII: VLAN CREES POUR LE 802.1X. 68
TABLEAU XIII : RESULTATS DES TESTS POUR UN ORDINATEUR SVF. 76
TABLEAU XIV : RESULTAT DES TESTS POUR UN TELEPHONE SVF. 77
TABLEAU XV: PLANNING DE MIGRATION DE L'ETAPE 1. 83
TABLEAU XVI: PLANNING DE MIGRATION DE L'ETAPE 2. 84
TABLEAU XVII : NOUVEAUX VLAN POUR LE 802.1X. 93

Etude et mise en œuvre du protocole 802.1x dans le cadre de la politique de sécurité de Sphéria Val de France. Mémoire d'Ingénieur C.N.A.M., Orléans 2013

RESUME

Dans un contexte de grande mutation que connaît le secteur des mutuelles et le caractère sensible des données de l'entreprise, la Direction du groupe Sphéria Val de France s'inquiète de sécuriser l'accès à son système d'information.
Alors que celui-ci est bien protégé des attaques extérieures, l'accès au réseau en interne ne l'est pas. Aujourd'hui, une personne mal intentionnée peut tenter de l'intérieur de l'entreprise d'accéder au réseau informatique depuis son ordinateur personnel.
L'objet de ce mémoire est donc d'étudier et de mettre en œuvre une solution permettant de contrôler l'accès physique au réseau de l'entreprise en garantissant l'identité des équipements afin de bloquer toute tentative d'intrusion.

Mots clés : 802.1x, EAP, RADIUS, système à authentifier, système authentificateur, serveur d'authentification, sécurité, réseau.

SUMMARY

In a context of deep changing on the complementary health insurance market and the sensitivity of its enterprise data, the executive management of Sphéria Val de France is concerned about securing access to its information system.
While it is well protected from external attacks, access to the internal network is not. Today, an ill-intentioned person can try, within the company, to access the local network from their own personal computer.
The purpose of this paper is to study and to implement a solution to control physical access to the corporate network by ensuring the identity of equipments to block any intrusion attempts.

Key words : 802.1x, EAP, RADIUS, supplicant, authenticator, authentication server, security, network.