Étude de la mise en place d'une solution de contrôle d'accès au réseau à travers le protocole 802.1X

Mamadou Bobo Diallo

CONSERVATOIRE NATIONAL DES ARTS ET MÉTIERS

PARIS

MÉMOIRE

Présenté en vue d'obtenir

Le DIPLÔME d'INGÉNIEUR CNAM

SPÉCIALITÉ : Informatique

Option : Réseaux Systèmes et Multimédia

Par

DIALLO Mamadou Bobo

Étude de la mise en place d'une solution de contrôle d'accès au réseau à travers le protocole 802.1X.

Soutenu le 11 Mai 2017

Jury

Président: Jean Pierre ARNAUD

Membres: Joëlle DELACROIX-GOUIN

Gino FLORICOURT

Christophe HACHEMI

Stéphane ROVEDAKIS

Remerciements

En préambule de ce mémoire, je souhaite adresser ici tous mes remerciements aux personnes qui m'ont apporté leur aide et qui ont ainsi contribué à l'élaboration de ce mémoire.

Tout d'abord je voudrais remercier mon tuteur CNAM, Jean Pierre ARNAUD, pour son implication, son suivi, son écoute et ses remarques judicieuses, qui m'ont permis de mener à bien ce mémoire.

Je tiens également à remercier le service Environnement Professionnel du secrétariat général des Ministères Économiques et Financiers pour m'avoir permis de réaliser ce mémoire dans de très bonnes conditions de travail.

Je remercie Georges KLEPATCH et Christophe HACHEMI, mes responsables au sein du bureau des infrastructures informatiques et télécommunications, pour leur disponibilité et leurs conseils tout au long de ce projet.

Je tiens à remercier également :

Fréderic ANDRIESSE, Alain DUBOIS, Gino FLORICOURT, Kheir-Eddine GHOUTI TERKI, Pierre LE GALL, Christian LEKIME, mes collègues, pour leur disponibilité et leur concours durant ce projet.

Enfin j'adresse mes plus sincères remerciements à tous mes proches et amis qui m'ont toujours soutenu et encouragé au cours de la réalisation de ce mémoire.

Glossaire

802.1x : standard permettant d'authentifier et d'autoriser l'accès au réseau à un équipement.

AAA : (Authentication, Authorization, Accounting) est un modèle sur lequel reposent les protocoles d'authentification. Il consiste en trois fonctions : l'authentification, l'autorisation et la traçabilité.

Authentification : Processus par lequel un système informatique s'assure de l'identité d'un utilisateur.

CLI : (Command Line Interface) interface en ligne de commande pour la prise de main sur les équipements réseau.

DHCP : (Dynamic Host Configuration Protocol) : permet la configuration automatique des paramètres réseaux d'une station (adresse IP, masque, passerelle, options diverses).

DNS : (Domain Name System) permet l'association d'une adresse IP à un nom de domaine, et réciproquement.

EAP : (Extenseible Authentication Protocol) protocole transportant les informations d'identifications des utilisateurs.

LAN : (Local Aera Network) est un réseau appartenant à une même organisation de petite taille.

LDAP : (Lightweight Directory Access Protocol) est un protocole permettant l'interrogation et la modification des services d'annuaire.

MAN : (Metropolitan Area Network) désigne des réseaux dont l'étendue est à l'échelle d'une ville.

NAS : (Network Access Server) est un client RADIUS faisant office d'intermédiaire entre l'utilisateur et le serveur RADIUS dans la transmission des informations d'authentification

OSI : (Open Systems Interconnection) est un modèle d'architecture proposé par ISO (Organisation internationale de normalisation) provenant directement du modèle de référence et développé dans le cadre des réseaux ordinateurs.

PEAP : (Protected Extenseible Authentication Protocol) protocole transportant les informations d'identifications des utilisateurs de manière sécurisée.

Proxy : solution permettant de filtrer et d'effectuer la demande (SMTP, HTTP, etc.) à la place du client.

RADIUS : (Remote Authentication Dial-In User Service) est un protocole client - serveur de la famille AAA permettant la centralisation des données d'authentification.

SSID : (Service Set IDentifier) nom du réseau sans fil (WiFi).

VLAN : (Virtual LAN) réseau virtuel permettant de segmenter un réseau local en plusieurs sous réseaux.

WAN : (Wide Aera Network) désigne des réseaux étendus sur plusieurs milliers de kilomètres.

WiFi : (Wireless Fidelity) ensemble de protocoles de communications sans fils utilisant les fréquences 2,4 et 5GHz. Ces réseaux sans fil font partis du WLAN (Wireless LAN).

1 Table des matières

2 Introduction

Les systèmes d'information occupent une place importante dans le fonctionnement des administrations publiques. Leur sécurité est un enjeu majeur pour l'État. Les investissements en matière de sécurité informatique sont de plus en plus indispensables.

En janvier 2011, lors d'un évènement majeur, les Ministères Économiques et Financiers ont subi une vaste attaque informatique. Cette attaque visant principalement les dossiers liés à cette manifestation, avait touché un certain nombre de postes informatiques.

À la suite de cette attaque, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), placée sous l'autorité du Secrétaire Général de la Défense et de la Sécurité Nationale[1], a proposé un ensemble de mesures pour améliorer la sécurité du système d'information des Ministères Économiques et Financiers.

Ce plan d'action était composé de 3 axes principaux :

- ✓ Renforcement de la sécurité au niveau des plateformes de services et des postes de travail ;
- ✓ Durcissement des règles de filtrage au niveau des équipements de sécurité, notamment pour la navigation internet ;
- ✓ Homogénéisation des pratiques en matière de sécurisation des systèmes.

La sécurité est un processus dont il faut continuer, tous les jours, à améliorer l'efficacité.

C'est dans ce contexte que mon mémoire s'inscrit. Il apporte une réflexion puis une solution pour renforcer le contrôle de l'accès aux réseaux informatiques des Ministères Économiques et Financiers grâce à la technologie 802.1X.

[1] L'ANSSI est un service à compétence nationale rattaché au Secrétaire général de la défense et de la sécurité nationale. Il a été créé par le décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information »

3 Objectifs de la sécurité

La sécurité en informatique peut être définie comme l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour assurer le bon fonctionnement d'un système informatique.

Il s'agit d'un ensemble de mesures et de bonnes pratiques mises en place pour le prémunir de tout risque pouvant dégrader ses performances. Pour cela, la sécurité répond à cinq objectifs principaux :

- ✓ Disponibilité : Garantir que les données et les services du système informatique sont disponibles pour les utilisateurs autorisés. C'est-à-dire mettre en place des dispositions pour protéger le système contre les attaques d'utilisateurs malveillants (déni de service »).
- ✓ Intégrité : Garantir que les données reçues et traitées n'aient pas été altérées pendant leur transmission ou leur traitement. C'est-à-dire s'assurer qu'elles n'ont pas été corrompues ou détruites.
- ✓ Confidentialité : Garantir que les informations ne soient accessibles qu'aux utilisateurs autorisés.
- ✓ Traçabilité : S'assurer que toutes les opérations réalisées par les utilisateurs peuvent être journalisées. Ainsi en cas d'enquête, grâce à aux identifications préenregistrées, on peut retrouver l'ensemble des informations liées à une activité.
- ✓ Non-répudiation : Garantir que les transactions effectuées ne puissent être niées.

Le système d'information est généralement défini par l'ensemble des données et des ressources matérielles et logicielles de l'organisation permettant de les stocker ou de les faire circuler. Il représente un patrimoine essentiel à la vie de l'organisation qu'il convient de protéger.

3.1 Les différentes méthodes d'attaques

Il existe plusieurs familles d'attaques n'ayant pas la même portée. Avant de les définir, nous les classons en deux types :

Les attaques multiples : elles sont généralement utilisées pour obtenir des privilèges afin de mener un autre type d'attaque. Les pirates vont, par exemple, prendre le contrôle d'une machine, et par rebond, étendre leurs privilèges avant d'attaquer un autre système.

Les attaques simultanées : nécessitent une coordination entre les pirates. Généralement, elles vont consister à utiliser les résultats de nombreuses attaques coordonnées et elles visent à saturer les cibles.

3.2 Profil des attaquants

Selon le rapport de l'ANSSI "Menaces informatiques" publié en 2006, les principaux motifs des attaquants sont l'appât du gain et l'avidité dans la majorité des cas. Ces deux facteurs sont amplifiés par les problèmes personnels et les jeux d'ego.

Avec le temps, la complexité des attaques informatiques augmente en même temps que les compétences techniques des attaquants diminuent. Ce rapport définit six profils différents d'attaquants :

Les agresseurs, sont communément appelés "hackers" ou encore "crackers" en fonction de leur dangerosité et de leurs objectifs. On utilisera le terme "Hacker" lorsqu'on sera confronté à des individus curieux, recherchant les failles de vulnérabilités d'un système ne cherchant pas obligatoirement à nuire. En revanche, les "Cracker" sont des individus dangereux exploitant des vulnérabilités afin de s'introduire dans les systèmes.

Les fraudeurs sont des individus cherchant à gagner de l'argent par tous les moyens. On les retrouve plus dans les activités de falsification de factures ou encore d'utilisation frauduleuse de cartes bancaires.

Les employés malveillants qu'on peut qualifier de fraudeurs internes sont des individus utilisant des moyens mis à leur disposition par l'organisation. Leur motivation peut être liée à la vengeance ou à un besoin financier.

Les militants sont des individus motivés par une idéologie ou croyance qui peuvent essayer de diffuser de l'information en masse. Dans le cas où ils accèdent au SI d'organisations en opposition avec leurs convictions, ils peuvent essayer de leur nuire.

Les espions sont des individus motivés par la guerre économique. Généralement ils travaillent pour une organisation concurrente. Leur personnalité est de nature discrète pour ne pas éveiller les soupçons. Leur but est de voler ou détruire des informations stratégiques de l'organisation qu'ils infiltrent.

Les terroristes généralement de personnalités motivées, ils aiment les actions spectaculaires à fort impact. Leur objectif est de faire parler d'eux. L'interconnexion et l'ouverture des réseaux ont favorisé l'extension de leur champ d'action.

Au-delà des profils que nous venons de définir, les motivations des pirates peuvent être diverses et variées en allant du ludique au stratégique.

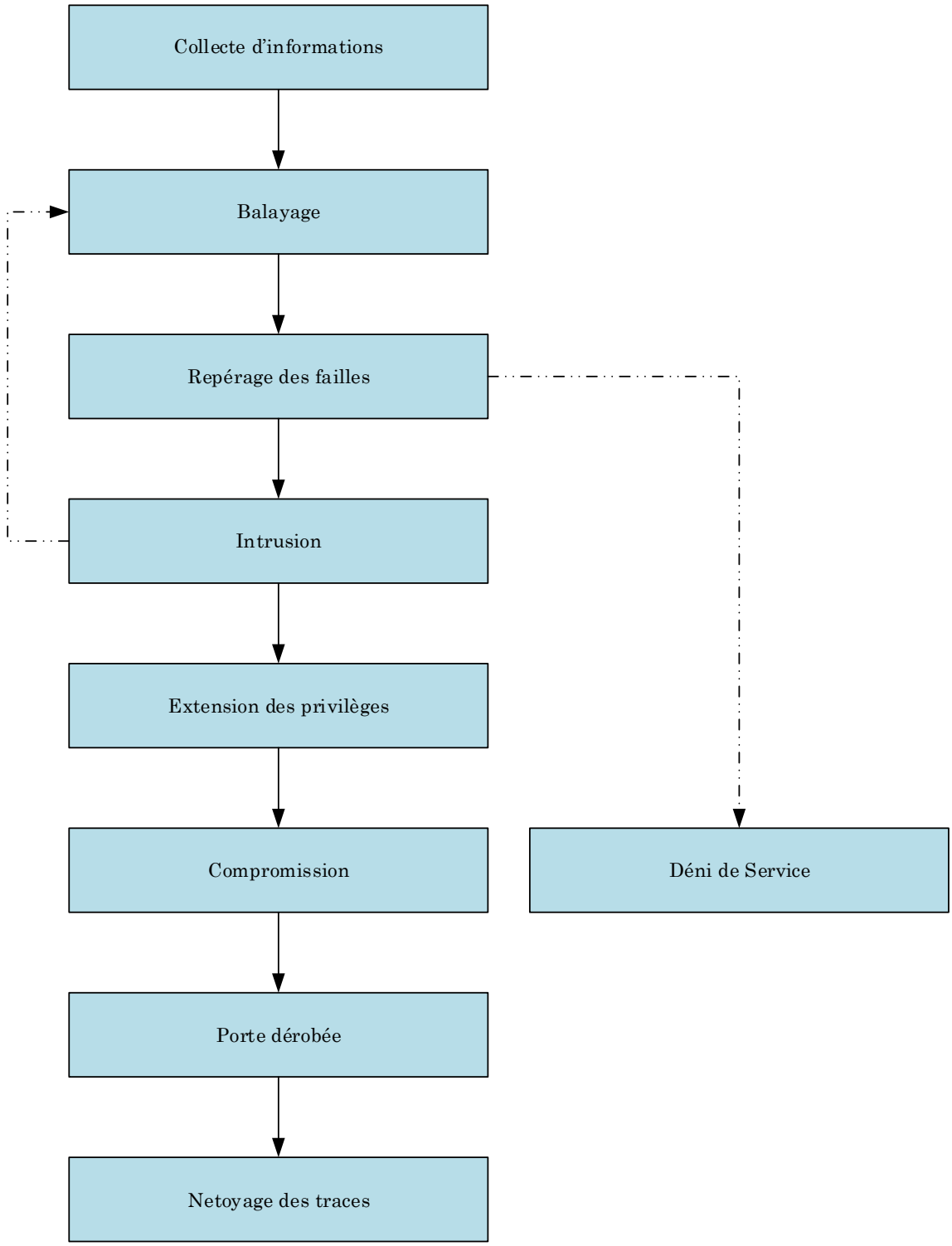
L'idée principale à retenir est qu'on n'a pas besoin d'être un spécialiste en informatique, pour corrompre un système informatique de façon illicite.

3.3 Méthodologie globale d'intrusion

Généralement, les pirates utilisent le même schéma de principe pour s'introduire dans un système d'information.

Ils vont commencer par inventorier l'ensemble des vulnérabilités du système en recherchant notamment celles qui existent déjà dans les protocoles, les systèmes d'exploitation, les applications et même l'organisation.

La figure ci-après, issue de l'article « Sécurité – Méthodologie d'une intrusion sur le réseau » rédigé par Jean François PILLOU[2] présente la cinématique globale utilisée pour s'introduire et corrompre un système d'information :



[2] Fondateur du site CommentCaMarche.net

Figure 1 Cinématique globale d'intrusion sur le réseau

La collecte d'information : Il s'agit de réaliser une prise d'empreinte de l'organisation. Cette phase va consister à recueillir le maximum d'informations disponibles sur internet (plages d'adresses IP publiques, structure de l'organisation, services activés,…).

Le balayage : Grâce aux informations recueillies à la collecte, cette phase va consister à identifier les adresses utilisées et repérer les ports ouverts[3] sur les machines.

Le repérage des failles : Cette phase utilise différents procédés allant de l'ingénierie sociale à la lecture de bannières. Avec l'ingénierie sociale, on va essayer de profiter des failles humaines, en approchant par exemple un utilisateur auquel on va essayer de soutirer des informations. Pour ce qui est des bannières, grâce aux informations issues de la phase balayage, on va essayer de se connecter sur les ports identifiés ouverts pour déterminer le type de service ouvert et la version des serveurs. À partir de cette phase, des attaques de type « déni de service » pouvant perturber la disponibilité du service peuvent déjà être lancées.

L'intrusion : Après avoir identifié l'ensemble des ressources, le pirate est en mesure de s'introduire dans le système pour le corrompre de l'intérieur. Cette phase va donc consister à repérer des comptes valides pouvant être utilisés. Pour cela, Il va consulter un annuaire ou mener des attaques de type force brute pour obtenir les mots de passe.

L'extension des privilèges : Ayant recueilli la liste des comptes valides, il va essayer d'augmenter les privilèges de ces comptes en tentant de s'octroyer les droits « administrateur ».

La compromission : une fois la cartographie des ressources réalisée et les privilèges des comptes étendus, le pirate va donc essayer d'étendre son champ

[3] Des outils tels que « Nmap » ou encore « Siphon » permettent de scanner le réseau en repérant les ports ouvert sur les machines.

d'action en tentant de compromettre le plus de serveurs possible. Cette phase va également consister à perturber les services offerts par le système.

La porte dérobée : Après avoir infiltré et réussi à compromettre le système d'information, cette phase va consister à créer une porte dérobée afin de revenir une autre fois reprendre la main sur le système. Il s'agit donc de créer, dans le système une faille de sécurité que seul le pirate connaîtra. Cette faille lui permettra, à sa guise, de revenir étendre son champ de nuisance dans le système.

Le nettoyage des traces : Le pirate va effacer l'ensemble des traces qu'il a laissées sur son passage en supprimant les fichiers qu'il a créés et en nettoyant les fichiers de journalisation. Il s'attachera à effacer uniquement les lignes d'activité qui concernent ses actions.

Une fois dans le système, il profite de ces vulnérabilités pour lancer une éventuelle attaque.

L'ensemble des phases que nous venons de décrire ci-dessus sont réalisées depuis l'extérieur ou l'intérieur de l'organisation. L'obtention des informations nécessaires à la réalisation d'intrusion depuis l'extérieur d'une organisation est très difficile. De plus en plus souvent, les pirates essaient d'exploiter les failles présentes à l'intérieur des organisations. La plupart du temps, l'accès au réseau filaire n'est pas contrôlé.

Les réseaux, étant au cœur du système d'information des organisations, sont exposés à des risques de type perte d'informations ou encore de type attaques contre lesquels ils doivent être protégés. La sécurité réseau est un processus à part entière entrant dans le plan global de sécurisation du système d'information.

4 Contexte

Je suis actuellement salarié en tant qu'Ingénieur Réseaux au sein de l'équipe Architecture et Surveillance des Réseaux du Bureau 1C « Infrastructures informatiques et Télécommunications ». Ce bureau fait partie du Secrétariat Général des Ministères Économiques et Financiers (MEF). Nous sommes en charge de la définition des architectures de réseaux de données, de l'exploitation et de la maintenance des infrastructures réseau.

Il convient de présenter le contexte organisationnel dans lequel le bureau se situe avant de présenter l'environnement technique dans lequel l'objet de ce mémoire est mis en œuvre.

4.1 Contexte Organisationnel

Le secrétariat général est l'entité transverse des MEF. Il convient de présenter son organisation et ses attributions.

4.1.1 Présentation du Secrétariat Général des Ministères Économiques et Financiers[4]

Le Secrétariat Général[5] des MEF assiste les ministres pour l'administration de leur ministère. Il est le garant du bon fonctionnement des services centraux.

En outre, le Secrétaire Général assiste les ministres dans l'exercice de leurs responsabilités de défense et de sécurité.

Le Secrétariat Général des MEF comprend :

[4] L'organisation du secrétariat général des ministères économiques et financiers est définie par l'Arrêté du 30 avril 2010 portant organisation du secrétariat général des ministères économiques et financiers.

[5] Les attributions du secrétaire général des ministères économiques et financiers sont définies par le Décret n° 2010-444 du 30 avril 2010 relatif aux attributions du secrétaire général du ministère de l'économie, de l'industrie et de l'emploi et du ministère du budget, des comptes publics et de la réforme de l'État et portant création d'un secrétariat général.

- ✓ La direction des ressources humaines ;
- ✓ Le service des affaires financières et immobilières ;
- ✓ Le service de la communication ;
- ✓ Le service de l'environnement professionnel ;
- ✓ La délégation à la modernisation ;
- ✓ La délégation aux systèmes d'information ;
- ✓ La délégation à l'encadrement supérieur.

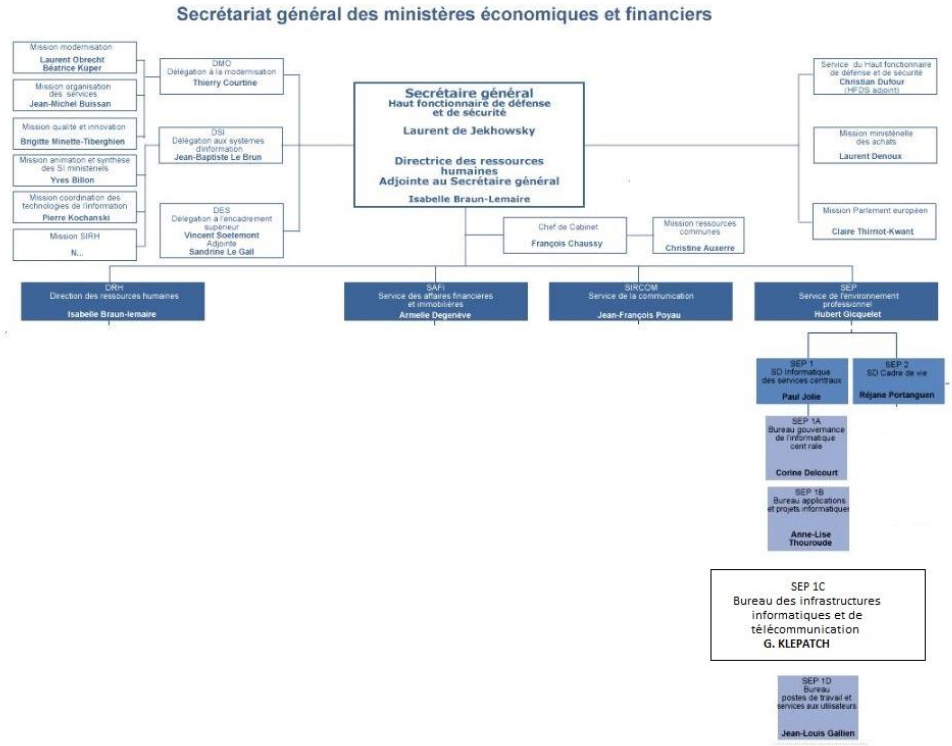


Figure 2 Organigramme du Secrétariat Général des Ministères Économiques et Financiers

4.1.2 Présentation du Service Environnement Professionnel (SEP)

Le SEP est une structure du Secrétariat Général des MEF. Le SEP a pour mission d'assurer la gestion des moyens des directions et des services de l'administration centrale des Ministères. En concertation avec les autres directions et services, il conçoit et met en œuvre :

- ✓ La politique immobilière de l'administration centrale,
- ✓ Les mesures et les moyens logistiques nécessaires au fonctionnement de l'administration centrale,
- ✓ La politique de développement des technologies de l'information, de l'informatique et du travail en réseau.

Comme le montre la figure 3, le SEP est composé de deux sous-directions :

- ✓ La sous-direction de l'informatique des services centraux : elle conçoit et met en œuvre pour les services centraux, et en concertation avec eux, la politique de développement des technologies de l'information, de l'informatique, de la téléphonie et du travail en réseau. Elle apporte conseil et expertise dans ces domaines. Elle coordonne et anime le réseau des correspondants informatiques. Elle assure l'équipement des services centraux ; elle met en place, exploite et administre les systèmes. Elle bâtit, gère et pilote les infrastructures de réseaux et de télécommunications.
- ✓ La sous-direction du cadre de vie : elle conçoit et met en œuvre la politique immobilière de l'administration centrale et assure l'exploitation et la maintenance de ses bâtiments et équipements. Elle est responsable de la sécurité et de la sûreté dans les bâtiments. Elle conçoit et met en œuvre les mesures et les moyens logistiques nécessaires au fonctionnement de l'administration centrale des ministères. Elle assure le service de traduction ministériel. Elle définit la politique documentaire et archivistique de l'administration centrale et gère ses ressources documentaires et ses archives.

La première sous-direction du SEP (SEP1), celle qui nous concerne ici, est en charge de la politique de développement des technologies de l'information, et coordonne la gestion de l'ensemble des moyens qui y sont consacrés. Pour la réalisation de ses missions, elle est dotée de quatre bureaux :

4.1.2.1 Le bureau 1A

Le bureau « Gouvernance de l'informatique centrale » élabore les orientations en matière d'informatique et de télécommunications des directions et services de l'administration centrale, en collaboration avec les directions et services. Il conduit la démarche qualité de la sous-direction. Il définit la politique de formation informatique des informaticiens et des utilisateurs des directions et services de l'administration centrale, en collaboration avec la sous-direction des ressources humaines. Il définit la politique d'achat informatique de l'administration centrale. Il est responsable des marchés informatiques des directions et services de l'administration centrale ainsi que des marchés ministériels qui lui sont confiés.

4.1.2.2 Le bureau 1B

Le bureau « Applications et projets informatiques » est responsable de la conception, de la réalisation, de la mise en place et du suivi des projets informatiques au profit des services de l'administration centrale. Il assiste les maîtrises d'ouvrage directionnelles et les conseille dans leurs choix d'investissement. Il réalise des études générales et analyse les besoins fonctionnels. Il assiste, conseille et forme les utilisateurs aux applications nouvelles. Il assure la maintenance et l'évolution des outils installés.

4.1.2.3 Le bureau 1C

Le bureau « Infrastructures informatiques et Télécommunications » met en place, exploite et administre les équipements centraux des directions et services d'administration centrale et les systèmes d'exploitation associés. Il construit, gère et pilote l'ensemble des réseaux informatiques, téléphoniques et audiovisuels des directions et services de l'administration centrale. Il en assure la qualité de service. Il assure l'interconnexion des systèmes informatiques des directions à réseau et l'interface opérationnelle avec les services interministériels. Il bâtit et met en service les architectures informatiques, optimise et surveille les infrastructures installées. Il conçoit et met en œuvre la politique de sécurité des systèmes d'information des directions et services de l'administration centrale.

4.1.2.4 Le bureau 1D

Le bureau « postes de travail et services aux utilisateurs » définit les configurations matérielles et logicielles de tous les postes de travail et périphériques installés dans les directions et services d'administration centrale. Il assure la maîtrise d'ouvrage et l'administration de la gestion du parc informatique matériel et logiciel des directions et services d'administration centrale ainsi que la gestion du catalogue des services rendus aux utilisateurs. Il assiste les utilisateurs des directions et services de l'administration centrale, en liaison avec les correspondants informatiques. Il coordonne et conseille les équipes du réseau des correspondants informatiques. Il assure, l'assistance informatique de proximité auprès d'unités de travail non dotées de correspondants informatiques. Il assure la régie audiovisuelle et répond aux besoins matériels et logiciels de manifestations organisées dans l'enceinte des bâtiments des services centraux du ministère.

4.2 Contexte technique

4.2.1 Architecture réseau des Ministères économiques et financiers

Le Bureau 1C est en charge de l'ensemble des réseaux des directions et des services de l'administration centrale. Ce périmètre comprend le site de Paris – Bercy[6], portant les plateaux informatiques du ministère, ainsi que 20 sites importants repartis sur la région île de France.

4.2.1.1 Architecture Physique

Le site de Bercy est composé de cinq bâtiments (Colbert, Vauban, Necker, Sully et Turgot).

[6] Nous remplacerons l'appellation Paris – Bercy par Bercy

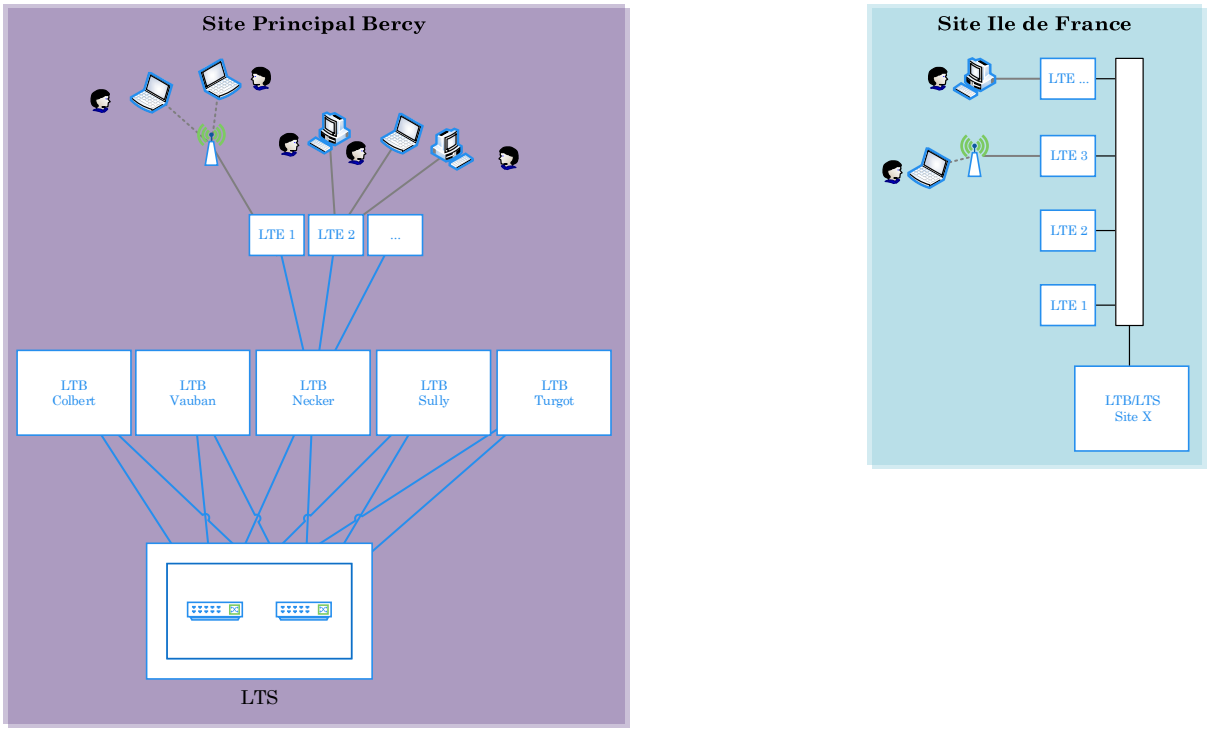


Figure 3 Architecture Physique des sites

Les utilisateurs sont raccordés au réseau à l'aide de commutateurs implantés dans une centaine de LTE (Locaux Techniques d'Étage). Les LTE sont reliés par des liaisons Gigabit Ethernet (1000 base SX ou LX) au commutateur central du bâtiment LTB (Locaux Techniques de Bâtiment) selon une topologie en étoile. Les cinq LTB sont raccordés par des liaisons Gigabit Ethernet à un commutateur de site (LTS).

Les autres sites d'Île de France sont raccordés selon une architecture similaire à celle du site de Bercy : Les LTE sont raccordés selon une topologie en étoile au commutateur central LTB qui fait office de LTS.

Les commutateurs des LTS, LTB et LTE sont des commutateurs de niveau 2 et 3 de marque HP, H3C et 3COM.

4.2.1.2 Infrastructure WAN (Wide Area Network)[7]

Au niveau WAN, les Ministères Économiques et financiers disposent d'un parc de liaisons utilisant les technologies suivantes :

[7] Les réseaux IPVPN, ECOTEL,

- ✓ IPVPN
- ✓ Ethernet « Any to Any » utilisant la technologie VPLS (Virtual Private LAN Service)[8]

L'architecture du réseau général du ministère est présentée par la figure ci-dessous :

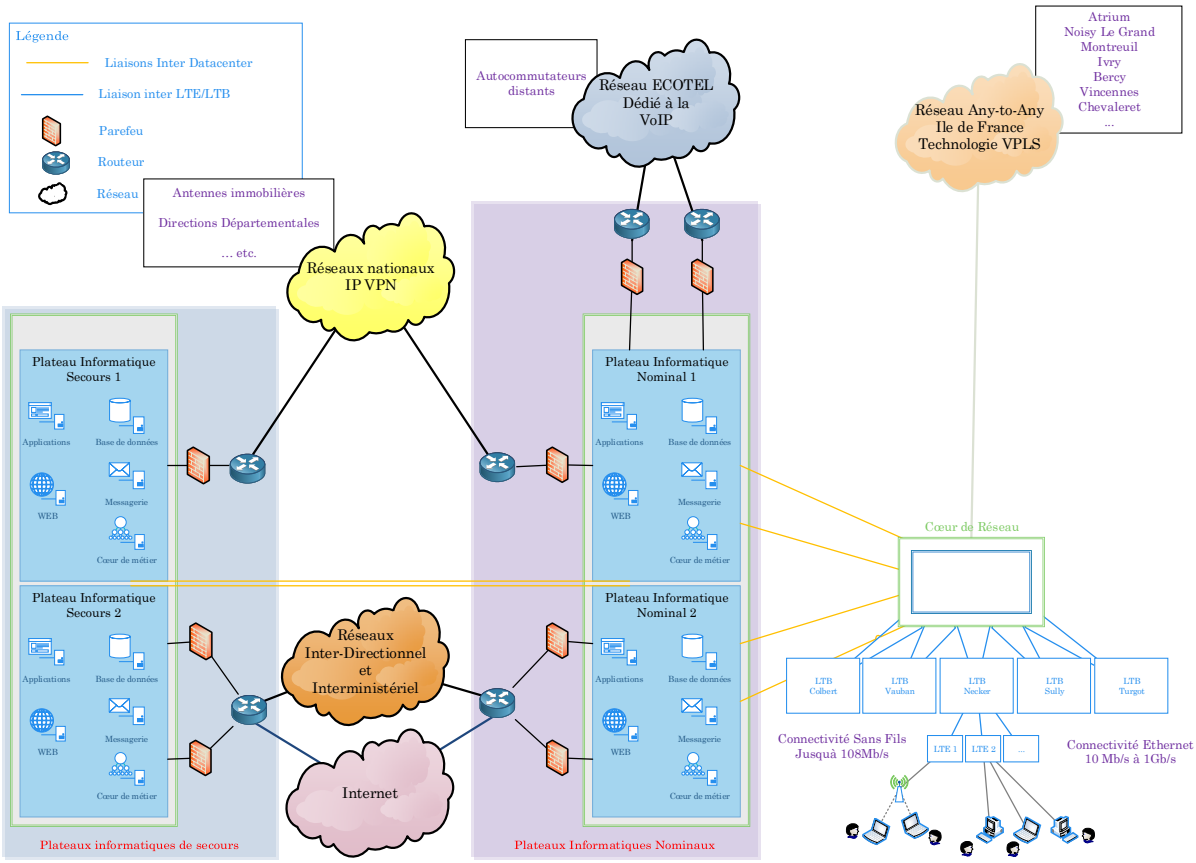


Figure 4 Infrastructure WAN des ministères économiques et financiers

Les plateaux informatiques représentent les Datacenter hébergeant le système d'information du ministère. Pour ce faire ils hébergent :

- ✓ Le réseau « Ecotel », un IPVPN dédié à l'interconnexion des autocommutateurs en Voix sur IP (VoIP).

[8] Le Virtual Private LAN Service est un service Ethernet multipoint-à-multipoint utilisant le protocole MPLS pour interconnecter des réseaux locaux de plusieurs sites distincts entre eux. Ces sites apparaissent donc au niveau logique comme faisant partie du même réseau local.

- ✓ Les réseaux IP VPN RG, dédiés à l'interconnexion des sites provinciaux appartenant aux Ministères Économiques et Financiers et des partenaires.
- ✓ Les réseaux interdirectionnels (RIDIR) et interministériel (RIE),
- ✓ Les accès internet du ministère

L'interconnexion des Ministères de l'état et des directions des MEF à travers les réseaux interdirectionnels et interministériels est réalisée par le Réseau Interministériel de l'État[9]. L'ensemble des réseaux IPVPN sont portés par le RIE.

4.2.1.3 Architecture Logique

Le réseau de Bercy est segmenté en plusieurs réseaux virtuels (VLAN), les principaux réseaux sont le « réseau général » qui regroupe de façon générique les VLANs des postes des utilisateurs, les réseaux dédiés aux plateaux informatiques, les réseaux dédiés aux cabinets ministériels.

À chaque réseau virtuel correspond un réseau IP. Les réseaux IP de l'Administration Centrale sont routés par les commutateurs de bâtiments (LTB) dans une Virtual Routing and Forwarding (VRF[10]) spécifique. Ceux des directions le sont dans leurs VRF respectives. Enfin, une VRF spécifique est utilisée pour l'administration des équipements.

4.2.2 Analyse des mesures de sécurité existantes

4.2.2.1 Les mesures existantes :

Un ensemble de mesures de sécurité ont été prises pour se prémunir contre les éventuelles attaques. Ainsi, au niveau réseau, les MEF sont protégés vis-à-vis des accès en provenance d'Internet par une DMZ à deux niveaux (Web et Données). Le secrétariat général se protège également des différentes directions qui composent les MEF par une série de pare-feu.

D'un point de vue utilisateurs, deux méthodes d'authentification coexistent en fonction des usages :

[9] Ici, il s'agit de l'entité en charge de la gestion du Réseau Interministériel d'Etat (RIE)
[10] Une VRF est un environnement de routage virtuel cloisonné des autres environnements.

- ✓ Les pare-feux permettent l'identification par adresse IP
- ✓ Le système d'authentification Single Sign On (SSO) permet l'authentification unique des utilisateurs pour l'accès aux applications web.

En ce qui concerne l'accès au réseau, le réseau filaire ne comporte pas de mesures de sécurité renforcées. En revanche, sur le réseau sans fils, des dispositions sécuritaires existent en fonction du service souhaité[11]. Les utilisateurs sont autorisés à se connecter en fonction de leurs profils :

- ✓ Les visiteurs des MEF ont un accès dédié avec un SSID « Bercy Invité ». En se connectant sur ce SSID, ils sont renvoyés vers une page d'authentification où ils doivent renseigner un login et mot de passe. Ces couples de login et mot de passe ont une durée de validité d'un jour. Ce SSID offre un accès à internet après avoir passé le processus d'authentification.
- ✓ Les agents du ministère utilisent le SSID « Bercy Intranet » pour accéder aux réseaux du ministère. Pour se connecter, ils doivent être munis d'une clé cryptographique contenant un certificat délivré par l'autorité de certification du ministère. Cette clé permet de monter un tunnel chiffré pour les échanges d'authentification et de vérifier l'identité de l'agent. Ce SSID offre à chaque utilisateur, en fonction des informations renseignées dans son profil au sein de l'annuaire l'accès à son environnement de travail. Un contrôle d'intégrité du poste de travail qu'il utilise est également effectué avant de lui accorder l'accès au réseau.

4.2.2.2 La Ligne Maginot : Un concept révolu

Pendant longtemps les organisations se sont protégées en utilisant le concept de la ligne « Maginot » c'est-à-dire en mettant une barrière entre le monde extérieur et le monde intérieur. Ce concept a montré ses limites, car comme l'évoquait Nicolas Six dans son article « Le danger vient de l'intérieur de la citadelle

[11] Deux services cohabitent au niveau du réseau sans fils : un service pour les personnes étrangères au ministère et un service pour les personnes travaillant au ministère.

informatique »[12], les équipements de sécurité existants permettent d'écarter la menace extérieure mais nullement les menaces et malveillances internes.

En effet, un utilisateur, qu'il soit employé, prestataire ou pirate, peut grâce à une prise brassée, connecter une machine infectée au réseau pouvant mettre en péril la santé de l'ensemble du système d'information. Il peut également organiser la fuite d'informations stratégiques si ses droits d'accès aux informations sont mal gérés.

L'idée qui résulte de cet article est de protéger l'utilisateur du SI contre les actes de malveillances qu'il pourrait effectuer à son insu et, par la même occasion, de dresser le plus d'obstacles possible sur le chemin des personnes mal intentionnées.

En général, les efforts sont faits pour la sécurisation des postes de travail, des serveurs et des applications. En complément de cela, nous devons être capables d'autoriser ou de refuser l'accès au réseau en fonction de critères bien définis.

En quelques chiffres, le secrétariat général des MEF est en charge de la gestion de :

- 8000 utilisateurs
- 560 commutateurs d'étage
- 70 équipements de sécurité

4.2.3 Expression du besoin

4.2.3.1 Le besoin

La Sous-direction Informatique du secrétariat général souhaite, pour l'année 2016, étudier l'opportunité de la mise en place d'un système d'authentification des utilisateurs lors de leur accès au réseau filaire. Cette solution, couvrant le

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

périmètre du secrétariat général[13], devra permettre d'identifier les utilisateurs et de les autoriser à accéder au réseau en fonction de leur profil. Elle devra être hautement disponible et redondée.

Le cycle de vie des technologies utilisées au sein des ministères étant lié aux marchés publics, la solution devra reposer sur des standards.

Un ensemble d'équipements informatiques différents composent l'environnement des MEF :

- ✓ L'ensemble de ces équipements sont reliés à des commutateurs de niveau 2 et 3. Ces commutateurs sont principalement de marques HP, H3C et 3COM.
- ✓ Les bâtiments sont équipés de badgeuses pour le pointage des agents. Des copieurs multifonction sont également disponibles à chaque étage.
- ✓ Les utilisateurs sont équipés de postes informatiques fixes ou portables. Une partie de ces utilisateurs sont équipés de téléphones IP de marque ALCATEL pour le service téléphonie.

4.2.3.2 Le planning

Le planning attendu comporte deux phases, une phase d'état de l'art des solutions d'authentification suivie d'une phase de déploiement.

Au cours de la phase d'état de l'art, les solutions du monde libre ainsi que celle du monde propriétaire devront être étudiées.

[13] Le secrétariat général a sous sa responsabilité l'ensemble des infrastructures des services centraux des Ministères Économiques et financiers.

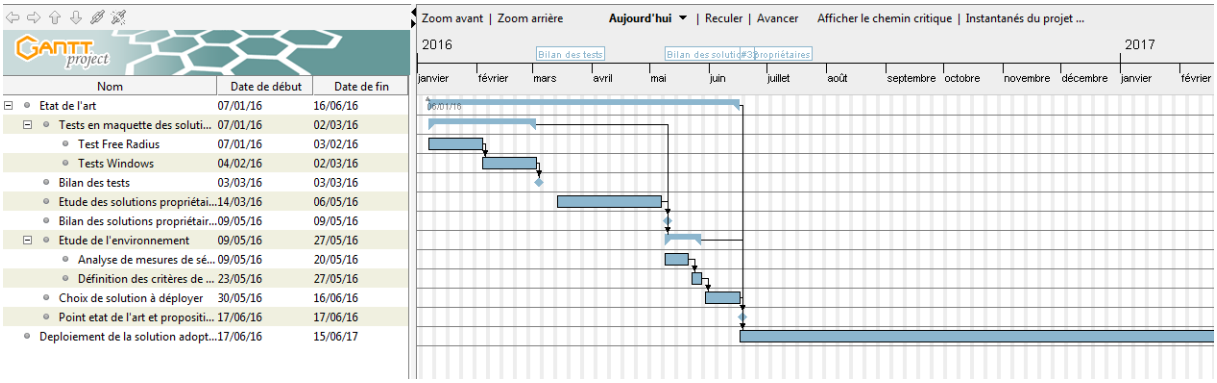


Figure 5 Planning général projet Contrôle d'accès au réseau

En fonction de la solution retenue, un planning de déploiement courant sur une année devra être proposé.

4.2.4 Spécifications

Le système d'information du ministère propose un ensemble de services à ses utilisateurs.

4.2.4.1 Exigences fonctionnelles

La solution doit permettre d'authentifier, de façon unique, l'accès des agents du SG et des personnels des cabinets ministériels au réseau du ministère. Sur le périmètre des salles de réunion, une authentification « visiteurs » pourra être mise en place.

D'un point de vue ergonomique, il est souhaité qu'elle puisse être adaptée afin de respecter la charte graphique des MEF. De plus, il serait appréciable que les informations affichées durant le processus de connexion soient interprétables par l'utilisateur lambda.

De même, il est souhaité que la cinématique de connexion, comme décrite par la figure ci-après, soit dynamique et ne donne pas l'impression que le processus de connexion soit figé.

D'un point de vue connectivité, il est souhaité que, en cas de perte de connexion, le délai de reconnexion automatique soit paramétrable ainsi que le nombre de tentatives. De plus, la durée maximale d'une session devrait être paramétrable.

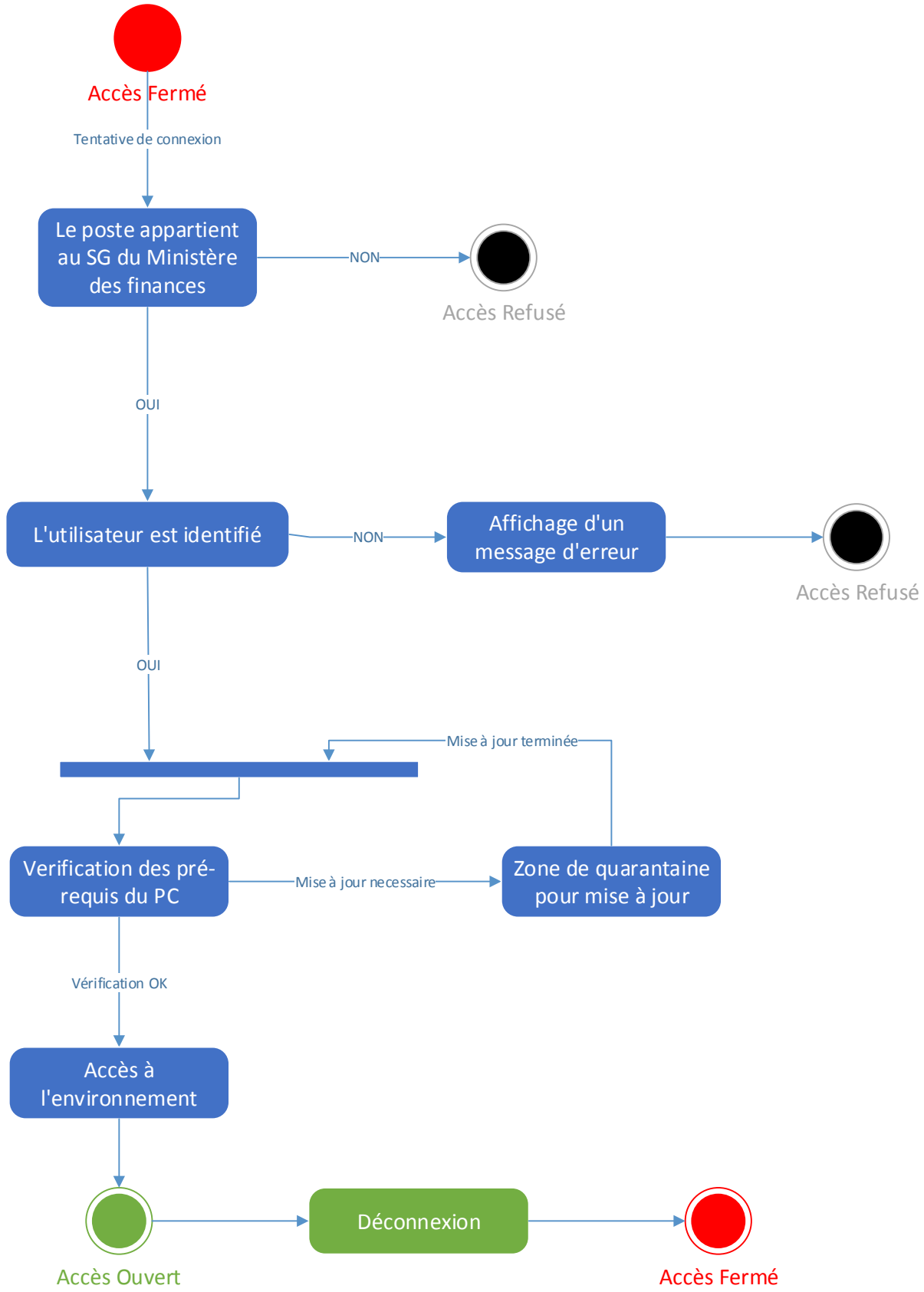


Figure 6 Cinématique de connexion au réseau

Conformément à la cinématique de connexion proposée ci-dessus, si le poste de travail identifié comme appartenant aux ministères tente de se connecter et qu'il n'est pas à jour, il est souhaité qu'il soit placé dans une zone temporaire lui permettant de faire les mises à jour adéquates avant de pouvoir accéder à l'ensemble des services.

4.2.4.2 Exigences de sécurité

Les postes de travail appartenant aux Ministères Économiques et Financiers devront être identifiés et soumis au processus d'authentification des utilisateurs.

Dans le cas contraire, la solution devra tout de même permettre d'authentifier les utilisateurs, soit par auto enregistrement, soit par parrainage.

Les flux d'authentification doivent être chiffrés entre le poste de travail et l'équipement de connexion.

La solution doit vérifier la conformité du poste :

- ✓ Vérifier la version de l'antivirus.
- ✓ Vérifier le niveau de mise à jour de l'antivirus, forcer la mise à jour si besoin.
- ✓ Vérifier le niveau de mise à jour de l'OS.
- ✓ Vérifier que le pare-feu du poste est bien actif, et si besoin faire les mises à jour de règles de filtrages.

La solution devra permettre d'associer les utilisateurs à des profils en fonction des informations se trouvant dans l'annuaire du ministère. Ces profils permettront d'accorder l'accès au réseau en fonction de l'emplacement.

Pour des besoins de traçabilité, la solution devra permettre à chaque client, ayant accédé au réseau, de disposer d'une adresse IP ayant un bail long terme auprès du serveur DHCP. Elle devra également tracer les évènements liés au processus d'authentification de l'utilisateur.

4.2.4.3 Exigences opérationnelles

La solution doit pouvoir être installée sur un environnement redondé sur un site principal et un site de secours. Elle doit permettre, en cas de défaillance du site principal, un basculement automatique vers le site de secours. Un réglage, pour permettre un basculement manuel est également souhaité.

L'architecture proposée devra être dimensionnée pour authentifier, en fonctionnement nominal, jusqu'à 10 000 utilisateurs.

La solution retenue doit être compatible avec Windows 7 et 10. Son intégration dans les environnements utilisateurs devra également être étudiée.

La solution devra disposer de fonctionnalités natives de reporting pour suivre l'activité des connexions. Elle devra permettre la personnalisation des messages d'erreurs, afin de faciliter le travail des équipes de support.

5 État de l'art : Le standard 802.1X et les protocoles EAP et RADIUS

802.1X est un protocole de contrôle d'accès au réseau (basé sur le contrôle du port) initialement proposé par IEEE pour sécuriser l'accès aux réseaux filaires de type Ethernet. Il est également utilisé pour sécuriser l'accès aux réseaux de type sans fils.

Ce protocole contrôle l'accès au réseau en authentifiant les machines qui se connectent sur les interfaces réseau d'un commutateur où la fonctionnalité est activée. Il s'agit d'un protocole fonctionnant en concert avec les technologies de type AAA (Authentication, Authorization and Accounting), principalement RADIUS. Ces technologies, offrant une plateforme uniforme pour le contrôle des accès, la gestion des autorisations et la journalisation des activités, offrent les fonctions de sécurité suivantes :

- ✓ Authentification : identifier un utilisateur et déterminer s'il est autorisé.
- ✓ Autorisation : attribuer des droits à l'utilisateur et contrôler son accès aux ressources et services (par exemple lui donner les droits en lecture sur l'état d'un service,…)
- ✓ Gestion de comptes : enregistrer toutes les informations liées à l'usage d'un service (type de service, début du service, trafic lié au service).

5.1 Le standard 802.1X

Le protocole 802.1X repose sur un modèle client-serveur. Pour son bon fonctionnement, nous avons besoin de 3 entités comme décrit dans l'illustration ci-après :

Le client : Un client souhaitant se connecter au réseau doit avoir un module 802.1x pour s'authentifier auprès du point de contrôle. Ce module est appelé supplicant.

Le point de contrôle : L'équipement d'accès au réseau va contrôler les droits du client. Il s'agit de l'authentifiant qui va jouer le rôle de contrôleur d'authentification (Network Access Controller [NAC]). Généralement, il se repose sur un serveur d'authentification pour réaliser cette tâche.

Le point de décision : Le point de décision fourni le service d'authentification au point de contrôle. Il authentifie les clients en fonction des informations qu'il reçoit. Ces informations sont des données émises par le point de contrôle. Le serveur en charge de la prise de décision, après avoir reçu et traité les données d'authentification, retourne au point de contrôle le résultat de l'authentification. En général, l'authentification peut être faite par un serveur de la famille technologique AAA. Il peut s'agir d'un RADIUS (Remote Authenticaton Dial in User Service), ou TACACS + (Terminal Access Controller Access-Control System) ou encore DIAMETER.

La technologie AAA la plus utilisée avec le protocole 802.1X pour authentifier les utilisateurs est RADIUS. Dans un petit réseau, la fonctionnalité d'authentification peut être assurée par le point de contrôle au réseau.

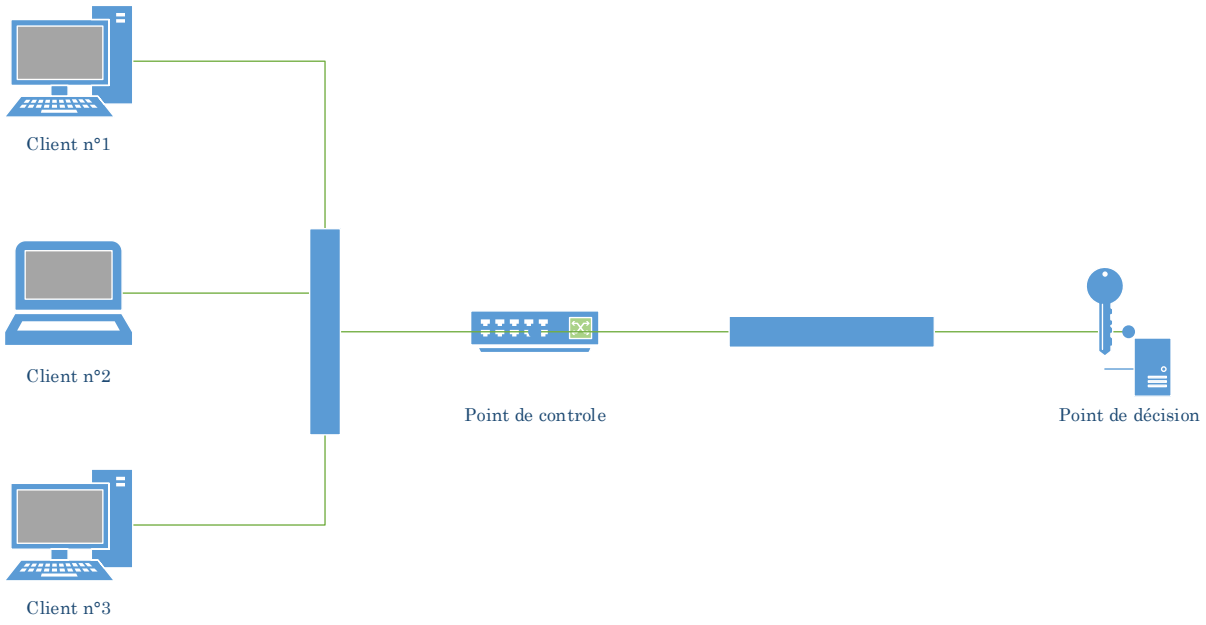


Figure 7 Architecture générale de fonctionnement 802.1x

5.1.1 Fonctionnement :

802.1X définit deux ports logiques pour l'équipement d'accès au réseau. Tous les paquets arrivant sur le port physique du point de contrôle sont visibles sur les deux ports logiques :

Port contrôlé : Le port contrôlé autorise les paquets entrants et sortants du port lorsqu'il est dans un état autorisé et il bloque le trafic lorsqu'il est dans un état non autorisé. L'état est autorisé lorsque le client a réussi son authentification et il est refusé lorsqu'il a échoué à l'authentification.

Port non contrôlé : Le port non contrôlé est toujours ouvert pour émettre et recevoir les trames Extensible Authentication Protocol (EAP) qui permettent les échanges d'authentification.

Dans un état non autorisé, un port contrôlé peut appliquer deux politiques :

Un contrôle bidirectionnel du trafic (paquets émis et paquets reçus par le client)

Un contrôle unidirectionnel du trafic (paquets émis uniquement)

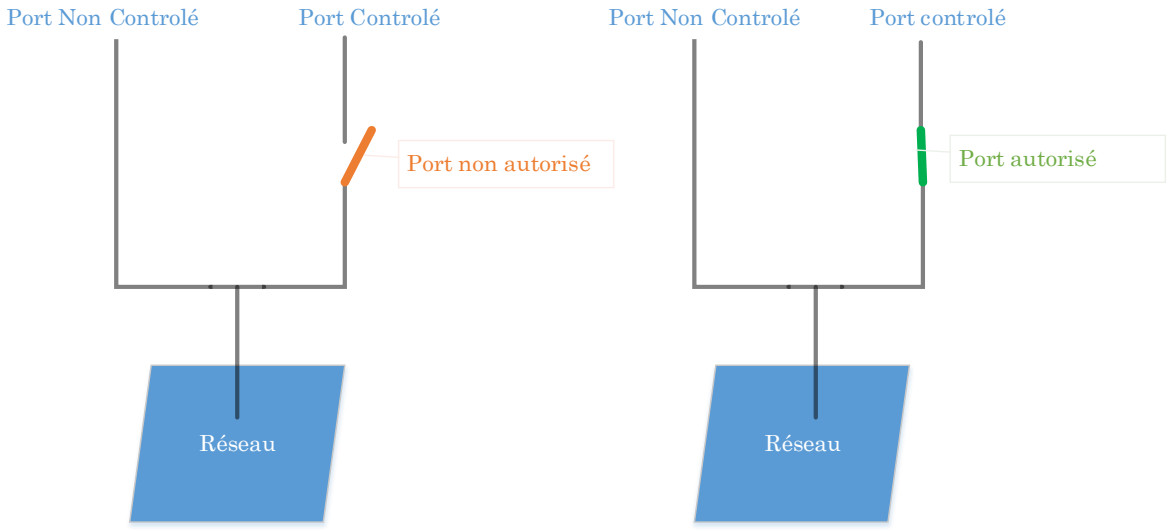


Figure 8 Les ports logiques en 802.1x

Pour son bon fonctionnement, le protocole 802.1x a besoin d'échanger des données avec les composants de son architecture. Pour cela, il utilise un protocole de transport de données d'authentification : Le protocole EAP.

802.1X utilise le protocole EAP (Extensible Authentication Protocol) pour transporter les paramètres d'authentification pour le client, le point de contrôle et le point de décision. Il utilise le modèle client-serveur et supporte un ensemble de méthodes d'authentification.

802.1X défini EAP over LAN (EAPOL) pour l'échange de paquets entre le client et le point de contrôle dans un réseau filaire et sans fils. Entre le point de contrôle et le point de décision, les paramètres sont transmis en utilisant EAP over RADIUS (EAPOR) qui encapsule les paquets EAP dans RADIUS

5.1.2 Le protocole EAP

Le protocole EAP, défini par les RFC 2284, 3748 et 5247, est un protocole de transport des données d'authentification reposant sur le modèle Client/Serveur. Historiquement, il a été créé pour permettre au protocole PPP (Point to Point Protocol) d'embarquer des méthodes d'authentifications d'accès au réseau[14]. Cependant il supporte l'ensemble des méthodes d'authentification.

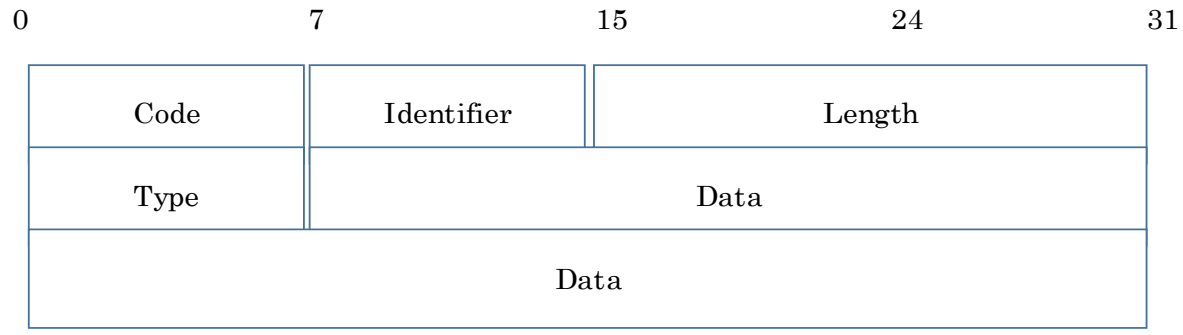


Figure 9 Structure d'une trame EAP

Comme décrit par l'illustration ci-dessus, une trame EAP contient cinq champs :

[14] Le protocole EAP a initialement été défini dans la RFC 2284 pour étendre les possibilités d'authentification avec le protocole PPP en 1998. Il a par la suite été défini en tant que protocole « standard » en 2004 dans la RFC 3748.

- ✓ Le champ « Code » : spécifie le type du message contenu dans la trame. Ce champ peut potentiellement comporter quatre valeurs. Chaque valeur correspond à un type de message possible lors des transactions EAP comme décrit dans le tableau ci-dessous :

Valeur	Description
1	Request
2	Response
3	Success
4	Failure

- ✓ Le champ « Identifier » : permet de corréler les trames de requête et de réponse l'équipement de connexion.
- ✓ Le champ « Length » : indique la longueur de la trame.
- ✓ Le champ « Type » : définit le type de protocole EAP utilisé (EAP MD5 ; PEAP ; EAP TTLS ; EAP TLS ;…)
- ✓ Le champ « Data » : contient, en fonction du champ « Type », les données transportées par la trame.

Pour son fonctionnement, il embarque de multiples méthodes d'authentification compatibles avec les différents types réseaux actuels (réseaux filaires, réseaux sans fils, réseaux PPP,…). Il reste extensible pour les méthodes d'authentification futures. Nous définissons les principales méthodes avec lesquels il est compatible :

EAP MD5-Challenge : L'authentification du client se fait par « login » et mot de passe. Pour valider l'authentification, le serveur utilise le mécanisme de défi réponse en envoyant une valeur aléatoire (le défi) au client. Ce dernier concatène cette valeur avec le mot de passe en utilisant l'algorithme de hachage MD5. L'empreinte obtenue est renvoyée au serveur qui, de son côté a également procédé au calcul de l'empreinte. Le serveur compare donc l'empreinte calculée avec l'empreinte reçue. Si les deux empreintes sont identiques alors l'authentification du client est acceptée sinon, l'authentification du client est

refusée. Cette méthode est peu utilisée de nos jours car les échanges entre le client et le serveur circulant en clair sur le réseau, elle est vulnérable aux attaques par dictionnaire hors ligne[15].

Protected EAP (PEAP) : Cette méthode, développée par Microsoft, RSA Security et Cisco Systems, est apparue pour pallier les carences d'EAP-MD5. Elle crée un canal crypté et sécurisé par la technique TLS. C'est le serveur qui détient un certificat qui va s'authentifier auprès du poste de travail du client. Avec le supplicant, il va monter un tunnel crypté pour authentifier l'utilisateur avec un couple login/mot de passe. Cette authentification se déroule donc en deux phases :

- ✓ Établissement du tunnel chiffré avec TLS entre le point de décision et le supplicant
- ✓ Authentification de l'utilisateur grâce aux informations recueillies par le supplicant avec un couple login/mot de passe.

Seul le serveur détient un certificat validé par une autorité de certification. Les clients doivent en revanche connaître l'autorité de certification et avoir installé le certificat de cette dernière.

EAP- Tunneled Transport Layer Security (EAP-TTLS) : Cette méthode a été développée par Funk Software. Elle crée un canal crypté et sécurisé par la technique TLS. Le serveur, détenant un certificat va s'authentifier auprès du poste de travail du client. Le supplicant, installé sur le poste de travail de l'utilisateur, authentifiera l'utilisateur par les différentes méthodes d'authentification disponible[16] généralement couple login/mot de passe.

EAP-Transport Layer Security (EAP-TLS) : L'authentification se fait à travers un tunnel chiffré de type SSL. Le serveur et le client doivent respectivement avoir un certificat qui leur est propre pour monter le tunnel de communication. Ces

[15] Un utilisateur malveillant pourrait capturer les échanges liés à une authentification réussie entre le client et le serveur en se mettant en écoute sur le réseau. Par la suite, il pourrait procéder à l'analyse de ces paquets hors ligne en tentant par exemple de retrouver le mot de passe grâce à un dictionnaire.
[16] L'authentification pourra être réalisée par le biais d'un couple login/mot de passe ou encore par le biais d'un certificat

certificats permettent d'authentifier le serveur et le client mais également de chiffrer les échanges entre ces derniers. Ils doivent être validés par une autorité de certification. Cette méthode peut s'avérer contraignante car elle augmente les échanges nécessaires pour l'authentification ce qui a un impact sur la durée d'authentification. Également, la nécessité d'avoir un certificat par machine peut s'avérer coûteuse à mettre en place et difficile à gérer lorsqu'on dispose d'un grand parc de postes utilisateurs[17].

L'étude portera sur le protocole RADIUS car :

- Il est un standard largement implémenté sur l'ensemble des équipements des constructeurs.
- Les équipes techniques en charge de l'exploitation des réseaux maitrisent cette technologie.
- Les MEF disposent de marchés permettant l'acquisition de matériels utilisant ce protocole.

5.2 Le protocole RADIUS

Le protocole RADIUS (Remote Authentication Dial-In User Service) a été développé à l'origine par Steve Willens pour la société Livingston Enterprises comme un serveur d'authentification et de gestion de comptes. Étant tombé dans le domaine public, il a été amendé par plusieurs RFC consécutives[18]. La version actuelle est définie par les RFC 2868. Il appartient à la famille des protocoles AAA (Authentication, Authorization, Accounting).

RADIUS est aujourd'hui le protocole d'authentification le plus utilisé et le plus implémenté sur les équipements réseaux. En effet, la plupart des constructeurs

[17] Il faut à chaque fois révoquer le certificat d'un poste de travail lorsqu'il quitte le parc et en créer un à chaque fois qu'un nouveau rejoint le parc. Toutes ces opérations doivent également être déclarées auprès de l'autorité de certification.
[18] La première normalisation a été celle énoncée par la RFC 2058 en 1997, elle fut modifiée dans la RFC 2138

ont développé leur propre bibliothèque de paramètres RADIUS[19]. Il est très déployé chez les fournisseurs d'accès internet pour l'authentification des connexions clientes. On l'utilise également pour l'authentification des accès distants sur les serveurs.

5.2.1 Fonctionnement:

Le protocole RADIUS fonctionne selon un modèle client-serveur : Les clients, souhaitant authentifier leurs utilisateurs, émettent des requêtes vers le serveur qui, après avoir réalisé la vérification de l'identité de l'utilisateur, renvoie une réponse.

Pour fonctionner, le protocole RADIUS utilise les ports 1812 et 1813 de la couche protocolaire UDP :

- ✓ Le port 1812 permet d'échanger les données liées à l'authentification des utilisateurs
- ✓ Le port 1813 permet la gestion de comptes pour assurer la traçabilité des opérations.

Le protocole RADIUS est donc un protocole d'authentification, de gestion de comptes (Accounting) mais pas d'autorisation. Pourtant, il fait partie de la famille des protocoles AAA (Authentication, Accounting, Authorization) grâce à sa grande extensibilité. En effet, la fonctionnalité d'autorisation peut être assurée à travers l'exploitation des attributs propriétaires développés par les constructeurs. Le protocole repose sur la transmission d'attribut Clef/Valeur, cette liste d'attributs n'étant pas limitée. Il est compatible avec la plupart des mécanismes d'authentification (LDAP, PAP, CHAP, MS-CHAP, EAP, LEAP,…).

Le client Radius, appelé NAS (Network Access Server), souhaitant authentifier ses utilisateurs partage un secret avec le serveur qui est en charge de l'authentification. Ce secret, servant de clef pour authentifier les transactions et

[19] Les principaux équipementiers ont développé leurs propres attributs (AvPairs) dans des librairies propriétaires (VSA : VendorSpecificAttributes).

effectuer le cryptage du mot de passe, n'est jamais transmis à travers le réseau. Le client effectue des requêtes Radius et agit en fonction des réponses reçues. Un serveur radius peut agir en tant que proxy radius pour d'autres serveurs Radius, ainsi que pour d'autres systèmes d'authentification (LDAP, SQL serveur,…).

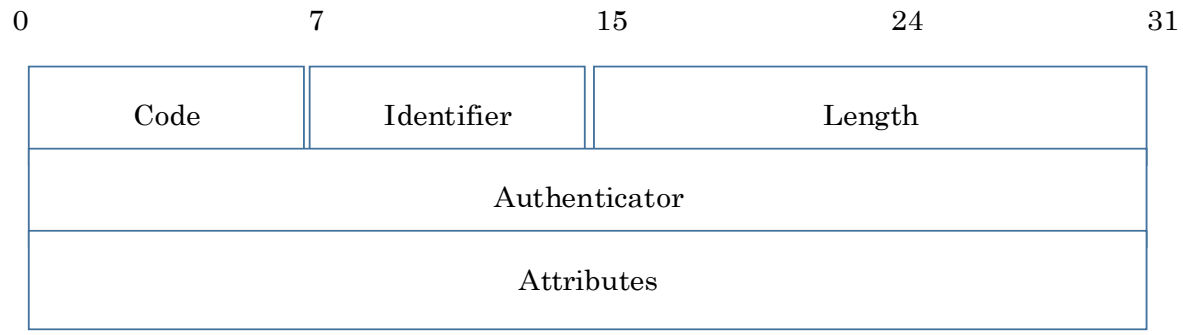


Figure 10Structure d'une trame RADIUS

Comme décrit par l'illustration ci-dessus, une trame RADIUS contient cinq champs :

- ✓ Le champ « Code » : spécifie le type du message contenu dans la trame. Ce champ peut potentiellement comporter neuf valeurs. Chaque valeur correspond à un type de message possible lors des transactions RADIUS comme décrit dans le tableau ci-dessous :

Valeur	Description
1	Access-Request
2	Access-Accept
3	Access-Reject
4	Accounting-Request
5	Accounting-Response
11	Access-Challenge
12	Status-Server (expérimental)
13	Status-Client (expérimental)
255	Reserved

- ✓ Le champ « Identifier » : permet de corréler les trames de requête et de réponse au sein des NAS (Network Access Server).

- ✓ Le champ « Length » : indique la longueur de la trame.
- ✓ Le champ « Authenticator » : authentifie les réponses du serveur RADIUS en utilisant le plus souvent un hachage MD5 du secret. Il permet aussi de préciser le mécanisme d'authentification de l'utilisateur à utiliser.
- ✓ Le champ « Attributes » : contient tous les tuples[20] d'attributs valeurs de la requête ou de la réponse. Il contient les données transportées par la trame.

Lors des échanges entre le client et le serveur, seuls le champ « identifier » et le champ « attributes » contenant le mot de passe sont cryptés. Le reste de la trame circule en clair sur le réseau.

5.2.2 La procédure d'authentification RADIUS

Pour qu'un utilisateur s'authentifie, Le NAS recevant la requête pour une connexion à distance, envoie une demande d'authentification au serveur Radius. Si l'utilisateur est accepté le serveur Radius autorise et détermine les services auxquels l'utilisateur peut accéder ainsi que des paramètres connexions.

Le schéma ci-après résume les échanges effectués lors d'une session RADIUS

[20] Un tuple est un néologisme basé sur le terme mathématique N-uplet. Il s'agit d'une collection ordonnée des valeurs d'un nombre indéfini d'attributs liés à un même objet.

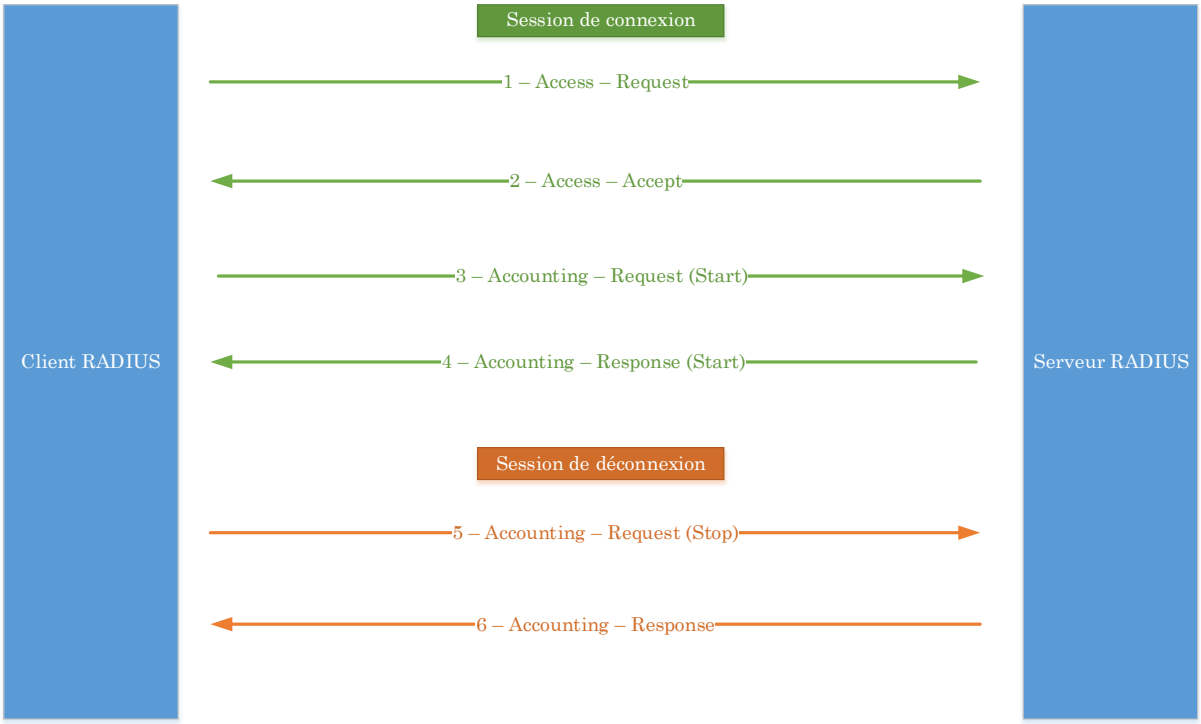


Figure 11 Séquence d'une session RADIUS

1. Le client envoie dans la requête « Access – Request » le couple « Login / password » crypté avec la clé partagée au serveur.

2. Le serveur compare la valeur reçue avec celle qu'il a lui-même calculée. Si le couple est valide, il renvoie un « Access – Accept »

3. Le client envoie dans la requête « Accounting – Request » les informations pour la gestion de comptes[21] (Accounting).

4. Le serveur répond lorsque les informations de comptabilité sont stockées.

5. Lorsqu'il se déconnecte, le client envoie dans la requête « Accounting – Request » les informations pour la gestion de comptes.

6. Le serveur répond lorsque les informations de comptabilité sont stockées.

[21] Comptabilité des opérations effectuées par le client.

5.3 Interopérabilité des technologies 802.1x, EAP, RADIUS

Le processus d'authentification 802.1x met en œuvre l'ensemble des protocoles 802.1x, EAP et RADIUS pour la réalisation de l'authentification.

5.3.1 Composition de l'architecture 802.1x

Le protocole 802.1X est utilisé pour les échanges entre le client et le point de contrôle. Pour authentifier un client, il se repose sur un point de décision généralement de type RADIUS. Le protocole RADIUS est utilisé pour les communications entre le point de contrôle (appelé NAS) et le point de décision. Le protocole EAP, grâce aux méthodes qu'il met à disposition, sera utilisé pour réaliser l'authentification entre le client et le point de décision.

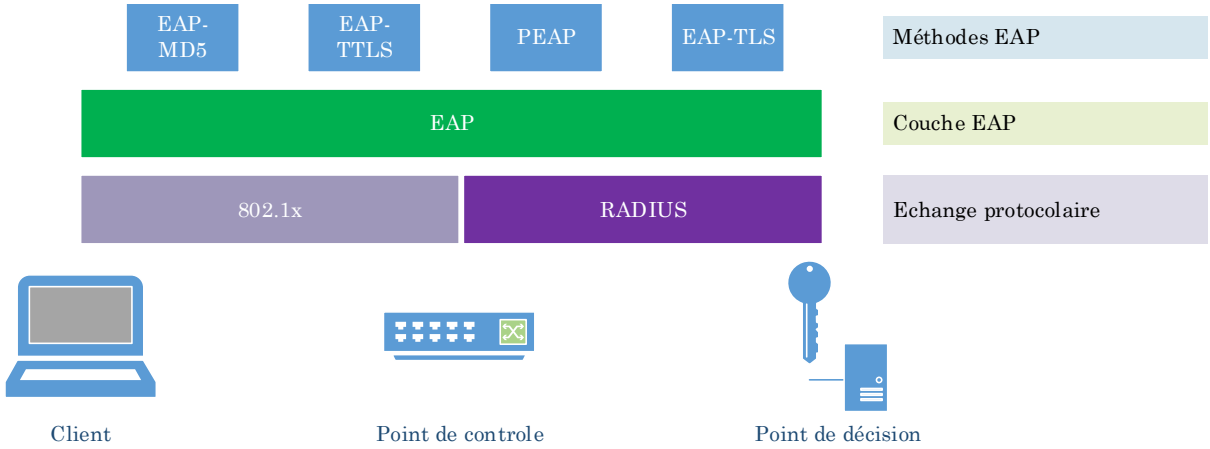


Figure 12 Les composants d'une authentification 802.1x

Le point de décision autorisera ou refusera l'accès du client au réseau à la fin du processus d'authentification. Il pourra également déterminer, grâce à ses attributs, le réseau (VLAN) dans lequel l'utilisateur devra être assigné.

Pour la prise de décision d'autorisation ou de refus d'accès, le point de décision (serveur RADIUS) peut se reposer sur un autre équipement d'authentification. Cet équipement d'authentification peut être un annuaire ou une base de données. Le point de décision utilisera donc le protocole particulier utilisé par l'équipement d'authentification (LDAP ou SQL) pour échanger des informations avec ce dernier.

5.3.2 L'authentification 802.1x

Le client, aussi bien que le point de contrôle peuvent lancer une authentification de type 802.1x.

Lorsque c'est le client qui initie le processus d'authentification, il envoie un paquet EAPOL-Start au point de contrôle. L'adresse MAC de destination de ce paquet est une adresse multicast spécifiée dans la norme IEEE 802.1X (01 : 80 : C2 : 00 : 00 : 03) ou à l'adresse MAC de Broadcast.

Le point de contrôle initie la procédure d'authentification lorsque le client ne peut pas envoyer de paquet EAPOL-Start (par exemple avec Windows XP). Pour cela, il fonctionne de deux manières :

Multicast : Le point de contrôle envoie en multicast toutes les 30 secondes un paquet EAP-Request

Unicast : en recevant un paquet avec une adresse MAC qui n'est pas dans sa table, il envoie un paquet EAP-Request pour demander l'identité. Il retransmet le paquet à intervalle régulier (à définir) lorsqu'il ne reçoit pas de réponse.

5.3.3 La procédure d'authentification 802.1X

Dans 802.1X, il y a deux approches pour l'authentification : EAP Relay et EAP termination. Le choix se fait en fonction des paquets EAP et des méthodes d'authentifications supportées par le serveur RADIUS.

Dans le mode EAP relay, défini dans la norme IEEE 802.1x, le client doit utiliser le même mode d'authentification que le serveur RADIUS. Sur le point de contrôle, on doit juste exécuter la commande "dot1x authentication-method eap" pour activer cette fonction.

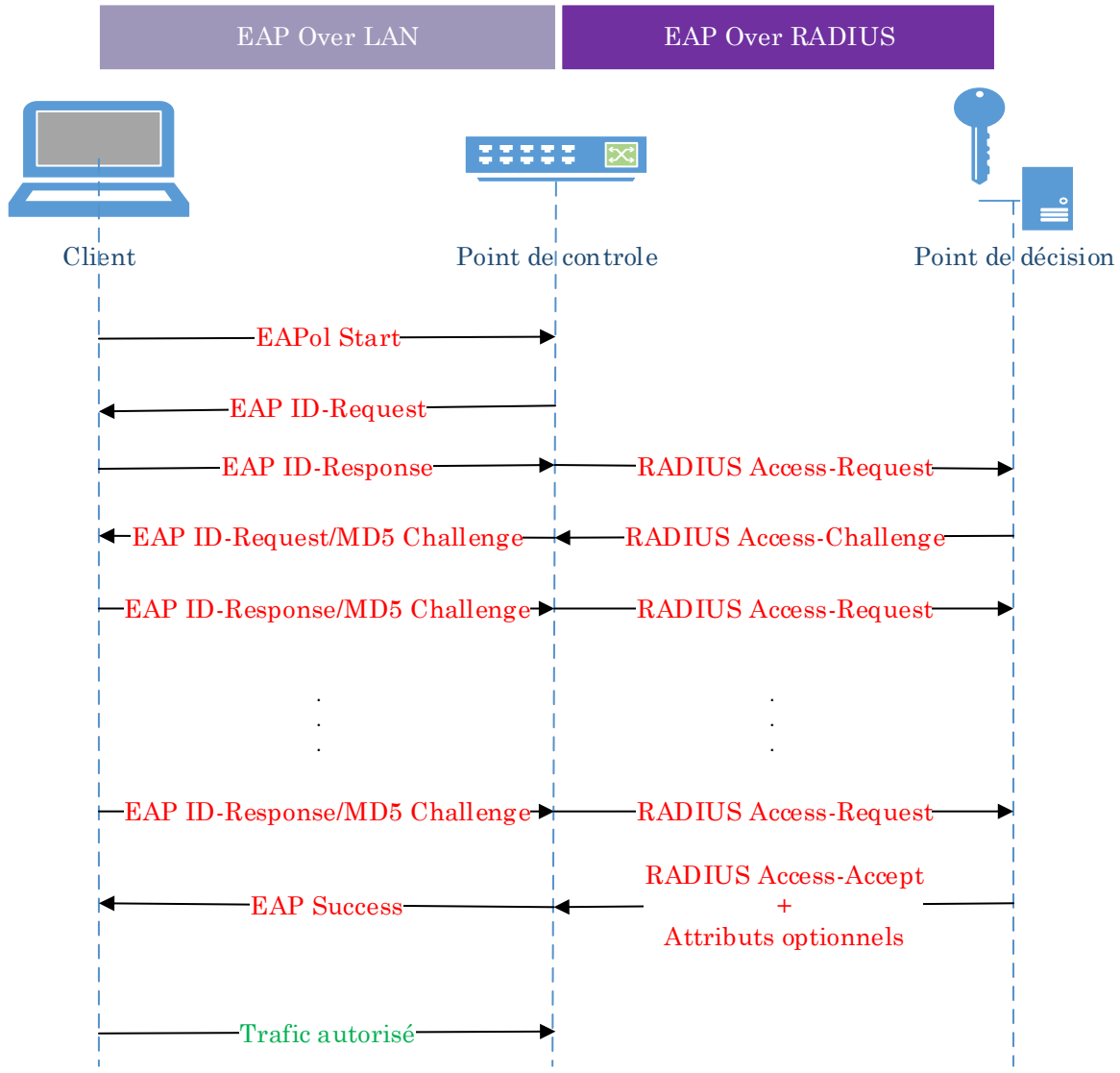


Figure 13 Procédure standard d'authentification 802.1x

6 Critères d'intégration

Le protocole 802.1x est un protocole de contrôle d'accès au réseau. Avec une solution embarquant ce type de protocole, un utilisateur peut se retrouver du jour au lendemain sans accès au réseau et aux services associés, notamment la téléphonie. Il est important dans un premier temps d'identifier l'ensemble des équipements connectés au réseau, de les classer par familles et de vérifier leur compatibilité avec les protocoles engagés.

Dans un second temps, à partir du résultat de l'identification, on va pouvoir déterminer quelle méthode retenir pour les différentes familles.

6.1 Identification des équipements à authentifier

Avant de définir les spécifications techniques nous devons identifier l'ensemble des équipements communiquant sur le réseau et nous assurer de leur compatibilité avec le standard 802.1x. Le cas échéant, il est important de proposer une méthode permettant de verrouiller la sécurité au niveau de la connexion de ces équipements.

6.1.1 Identification des équipements connectés sur le réseau

L'inventaire des matériels autorisés à se connecter au réseau selon les recommandations de notre PSSI révèle les informations présentent dans le tableau ci-après :

	Compatibilités			
Equipements	EAP - MD5	PEAP	EAP - TTLS	EAP - TLS
Ordinateurs portables	X	X	X	X
Téléphones IP	X			X
Ordinateurs fixes	X	X	X	X
Imprimantes	X			X
Badgeuses				

Tableau 1 Inventaire des matériels autorisés à se connecter au réseau

6.1.2 Proposition pour les équipements ne rentrant pas dans le périmètre de l'authentification 802.1x

Par souci d'efficacité, nous avons décidé d'exclure du champ de l'authentification quelques familles de machines.

Le tableau ci-après indique le mode de vérification adopté pour chacun d'entre eux.

	Compatibilités				Mode d'authentification		
Equipements	EAP - MD5	PEAP	EAP - TTLS	EAP - TLS	Parametage spécifique	Durcissement adresse MAC	Exclu
Ordinateurs portables	X	X	X	X	X		
Téléphones IP	X			X			X
Ordinateurs fixes	X	X	X	X	X		
Imprimantes	X			X		X	
Badgeuses						X	

Tableau 2 Solution retenue pour l'authentification des matériels connectés au réseau

Le choix que nous faisons est de se concentrer sur l'identité de l'utilisateur. L'ensemble des postes utilisateurs ayant une configuration spécifique, nous allons nous en servir pour les identifier.

Les imprimantes et les téléphones IP bien que compatibles avec la technologie 802.1x sont liés à des marchés d'exploitations spécifiques. Cela ne permet pas

d'avoir les marges de manœuvres suffisantes pour déployer la technologie 802.1x immédiatement.

Ainsi, pour les badgeuses et les imprimantes, nous mettons en place un mécanisme de durcissement d'accès. Le commutateur après avoir appris l'adresse MAC de l'appareil, bloquera toute autre tentative de connexion sur le port avec un appareil portant une autre adresse MAC.

Pour ce qui est des téléphones IP, ils ne seront pas authentifiés. Ils sont authentifiés par une l'infrastructure dédiée à la téléphonie.

Nous allons identifier les postes utilisateurs grâce à un paramètre spécifique. Cette pratique est conforme aux règles d'ingénieries définies par la PSSI du secrétariat général des MEF.

Les téléphones IP sont exclus car ce sont des équipements déjà authentifiés via l'infrastructure de téléphonie

Les badgeuses et les imprimantes auront un durcissement de la sécurité au niveau des ports des commutateurs sur lesquels elles sont connectées.

6.2 Spécifications Techniques

Dans cette partie, nous essayons d'apporter une réponse technique aux différentes exigences fonctionnelles évoquées.

6.2.1 Authentification des utilisateurs

Le choix qui a été fait au sein des MEF par la politique de sécurité est d'identifier les utilisateurs. Pour cela nous allons utiliser le service annuaire LDAP.

Deux moyens sont privilégiés pour l'authentification des utilisateurs :

- ✓ Le couple login et mot de passe de l'annuaire
- ✓ Le jeton cryptographique

Nous verrons plus loin que le choix de la méthode d'authentification de l'utilisateur se fera en fonction de son profil.

6.2.2 Exigences techniques de sécurité

Il n'y a pas de lien entre le poste utilisateur, et l'utilisateur final. Nous allons, dans la plupart des cas, vérifier uniquement que le poste appartient bien au parc des MEF avant de lui accorder l'accès au réseau.

Lorsque le poste n'appartient pas au parc des MEF, nous pourrons considérer dans certains cas qu'il s'agit d'un poste d'un visiteur. La stratégie d'authentification sera alors différente. Il sera alors automatiquement redirigé, lorsqu'il tentera de se connecter en salles de réunion et que son poste n'a pas la fonctionnalité 802.1x activée, vers un réseau visiteurs lui accordant un accès à internet. On proposera aux utilisateurs un autre moyen de s'authentifier. Cependant, dans la plupart des cas, l'accès est refusé.

La vérification de la conformité du poste est réalisable avec un supplicant installé sur le poste de l'utilisateur. En revanche, il n'existe pas de standard définissant le protocole à utiliser pour réaliser cette opération. Ainsi, quel que soit le supplicant utilisé, le protocole mis en œuvre pour vérifier la conformité d'un poste utilisateur vis-à-vis d'une politique de sécurité sera un protocole propriétaire.

Pour répondre aux exigences émises par la politique de sécurité, nous allons mettre en place un ensemble de Vlan dit de « quarantaine ». Ces Vlans permettront aux utilisateurs ayant échoué à la phase de vérification de la conformité du poste, de pouvoir réaliser les différentes mises à jour nécessaires avant de s'authentifier à nouveau.

Nous retenons deux méthodes pour authentifier les utilisateurs :

- Le couple login et mot de passe de l'annuaire : actuellement utilisé par l'ensemble des utilisateurs pour les ouvertures de sessions sur les postes de travail.
- Le jeton cryptographique : pour renforcer la sécurité au niveau de l'accès au réseau d'administration des équipements.

Nous mettons en place des réseaux de quarantaines pour les utilisateurs dont les postes de travail ne répondent pas aux exigences de sécurité.

6.3 Architecture Technique souhaitée

Nous proposons dans cette partie une comparaison des différentes méthodes d'authentification EAP avant de faire un choix technique. Puis nous présentons le modèle architectural sur lequel devra reposer la solution attendue.

6.3.1 Comparaison des méthodes d'authentification

L'authentification des utilisateurs se fera à partir d'une des méthodes évoquées lors de la définition du protocole EAP. Le tableau ci-après récapitule ces différentes méthodes et présente les avantages et inconvénients de chacune d'entre elles.

Type EAP	Login / mot de passe	Certificat	Implementation facile	Authenti Cryptée	Authentification mutuelle	Gestion simplifiée	Absence de certificat client		
EAP - MD5	🟢	🔴	🟢	🔴	🔴	🟢	🟢		
PEAP	🟢	🟢	🔴	🟢	🔴	🟢	🟢		
EAP - TTLS	🟢	🟢	🔴	🟢	🔴	🟢	🟢		
EAP - TLS	🔴	🟢	🔴	🟢	🟢	🔴	🔴		

Tableau 3 Comparaison des différentes méthodes EAP

La politique globale d'authentification sera EAP-TTLS. On privilégie le type d'authentification EAP-TTLS car il offre le choix de combiner différentes méthodes d'authentification.

Le canal d'échange des données d'authentification étant crypté, on pourra, en fonction des populations concernées, décliner une méthode d'authentification spécifique. Un utilisateur lambda utilisera son login et mot de passe habituel, tandis qu'un utilisateur faisant partie des équipes d'exploitation utilisera le certificat client qui lui aura été mis à disposition au préalable par l'administration.

6.3.2 Présentation de l'infrastructure attendue

L'infrastructure devra être redondée et secourue.

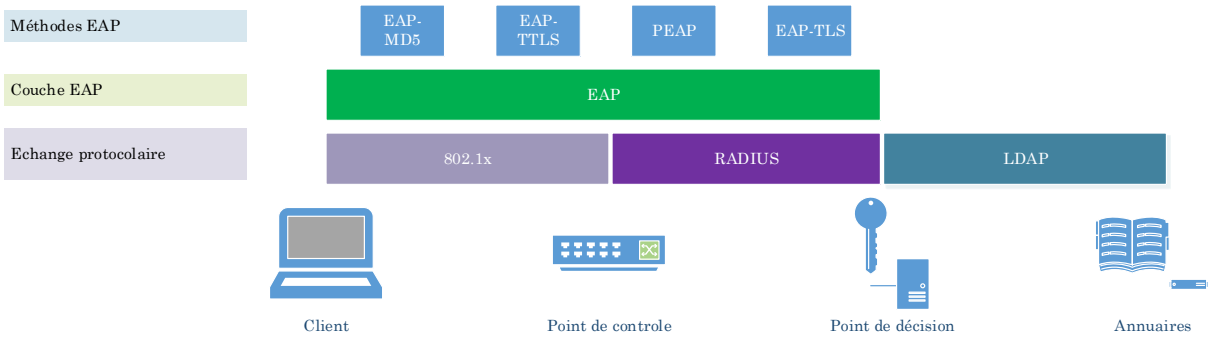


Figure 14 Infrastructure attendue

Le point de décision sera composé de deux nœuds dont un maître et un esclave. Ainsi, si un nœud tombe en panne, le service pourra automatiquement basculer sur le second nœud qui sera donc le nouveau maître.

Dans la configuration des commutateurs faisant office de point de contrôle, nous renseignerons les adresses IP des nœuds.

On utilisera un annuaire pour réaliser l'authentification des utilisateurs.

Nous choisissons le type EAP – TTLS pour authentifier les utilisateurs en 802.1x. Il permet d'authentifier l'utilisateur soit par le couple login / mot de passe soit par le jeton cryptographique.

7 Choix de solution de contrôle d'accès

7.1 Les critères

Il est important de définir un ensemble de critères pour faire des choix objectifs.

7.1.1 Critères Techniques

D'un point de vue technique, il est attendu que la solution retenue repose sur des standards du marché : elle doit pouvoir s'intégrer dans des environnements multi-constructeurs.

Pour l'authentification, la solution devra être compatible avec les différentes technologies d'annuaires. En effet, les MEF disposent d'un annuaire central utilisant la technologie LDAP. D'autres directions ont une latitude sur les technologies d'annuaires qu'elles utilisent. Par exemple, le secrétariat général utilise un annuaire Active Directory. Toutes les informations sont fédérées dans l'annuaire central.

En fonction du périmètre du projet, on se laissera le choix de faire reposer l'authentification soit sur l'annuaire LDAP central, soit sur l'annuaire Active Directory du secrétariat général.

7.1.2 Critères d'environnement

Au niveau de l'environnement, l'écosystème des MEF étant très complexe, la solution doit pouvoir s'intégrer dans cet écosystème.

La problématique du contrôle d'accès est déjà traitée par différentes solutions qui existent déjà dans l'environnement du ministère sur des périmètres spécifiques :

- ✓ Le contrôle de l'accès distant VPN est assuré par la solution NETWORK CONNECT de la société Juniper.
- ✓ Le contrôle de l'accès au réseau sans fil est assuré par la solution JUNIPER

Plusieurs solutions de contrôle d'accès étant en cohabitation, la solution retenue devra pouvoir facilement s'intégrer dans cet environnement.

L'idéal serait d'adopter une solution qui sera également capable de prendre en charge l'environnement sans fil. Ainsi, on pourra avoir une approche globale en matière de politique de contrôle d'accès aux réseaux filaires et sans fils. De plus, les coûts en matière d'investissement, d'exploitation et de maintenance se verraient optimisés.

L'authentification des utilisateurs reposera sur les annuaires LDAP présents dans les infrastructures des MEF.

7.2 Les solutions du marché

La problématique de la sécurisation des accès a été rapidement rencontrée dans les réseaux sans fils. En réponse à ce besoin, un ensemble de solutions a été développé aussi bien par la communauté du monde du libre que par les constructeurs. Dans cette partie, nous essayons de présenter quelques solutions provenant des deux univers et utilisant les standards.

7.2.1 Solutions Libres

Dans le monde du libre, deux technologies sont souvent utilisées :

7.2.1.1 FreeRadius

Free Radius est une implémentation gratuite et open source de serveur RADIUS dont le développement a commencé en 1999. Il ne s'agit pas d'une solution de contrôle d'accès à proprement parler mais plutôt d'une solution d'authentification compatible avec les protocoles EAP et la technologie 802.1x. Elle reste l'implémentation la plus utilisée dans le monde pour les solutions d'authentification.

Elle est compatible avec des systèmes d'exploitation de type Linux et offre une large gamme de possibilités d'intégration dans la plupart des architectures existantes. Compatible avec la plupart des protocoles d'authentification (802.1x, EAP,…), elle est associable à toute sorte de base d'authentification (LDAP, Annuaire Windows, MySQL, Oracle, PostgreSQL, DB2, fichier plat).

Pour avoir testé Free Radius en maquette, sa configuration consiste à paramétrer un ensemble de fichiers dans le répertoire /etc/raddb. Ce répertoire contient des fichiers commentés permettant de s'approprier les différents mécanismes et accompagnant la configuration. On y retrouve notamment :

Le fichier Clients. conf qui va déclarer les clients Radius ou NAS qui pourront communiquer avec le serveur et les secrets partagés associés.

Le fichier Users qui est une base de données locale qui va servir de base d'authentification des utilisateurs.

Le fichier Radiusd. conf qui regroupe un ensemble de paramètres dans le but de décrire un type de fonction souhaité. C'est dans ce fichier que sera paramétré le mode de fonctionnement de notre serveur RADIUS.

7.2.1.2 PacketFence

PacketFence est un logiciel gratuit et open source de contrôle d'accès au réseau. Compatible avec un grand nombre de constructeurs, il offre une interface qui permet d'agréger un ensemble de fonctionnalités telles que : le portail captif, la gestion centralisée des réseaux filaires et Wifi, une interopérabilité avec le protocole 802.1x, la détection de vulnérabilités, les sondes IDS permettant de détecter les intrusions.

Il est compatible avec des systèmes d'exploitation de type Linux et a besoin d'un ensemble de composants pour son fonctionnement :

Un serveur Web (Apache)

Une base de données (MySQL)

Un serveur RADIUS (FreeRadius)

Un serveur DHCP

7.2.2 Solutions Propriétaires

La plupart des constructeurs ont développé leur propre solution de contrôle d'accès au réseau. En général, les solutions qu'ils proposent apportent une réponse globale sur les problématiques de contrôle d'accès au réseau (Accès distant, Accès Filaire, Accès sans fil). Nous en étudions ici quelques-unes.

7.2.2.1 Network Policy Server

Depuis la version 2008 de Windows Server, Microsoft a développé un module permettant de gérer un service de stratégie d'accès au réseau. Il s'agit d'un rôle, que peut porter un serveur faisant partie du domaine, offrant une solution de contrôle d'accès à distance via réseaux privés virtuels (VPN), de contrôle d'accès aux réseaux filaires et sans fils.

Cette fonctionnalité permet de définir et d'appliquer des stratégies d'authentification et d'autorisation d'accès pour l'ensemble des utilisateurs d'un domaine Active Directory. Pour son fonctionnement, elle repose sur trois composants :

- ✓ Protection d'accès au réseau (NAP) : permet de s'assurer que les ordinateurs clients du réseau répondent aux exigences définies en matière d'intégrité par l'administrateur. Il va par exemple permettre de vérifier que l'ordinateur client dispose bien d'un antivirus installé et à jour. Pour fonctionner, il a besoin d'un supplicant ou que le supplicant intégré aux ordinateurs Windows soit activé.
- ✓ Le serveur Network Policy Server (NPS) : réalise, de façon centralisée, l'authentification et l'autorisation pour les connexions d'accès à distance, les connexions sans fils et filaires. Il est au cœur de l'architecture Microsoft et va permettre de définir et d'appliquer les différentes stratégies en fonction de la nature de la connexion.

- ✓ Le service routage et accès à distance : fournit l'accès aux ressources situées sur le réseau privé aux utilisateurs à distance. Il s'agit d'un composant qui va permettre de monter des tunnels VPN entre les différents utilisateurs à distance et le réseau privé de l'organisation.

7.2.2.2 ClearPass

ClearPass est une solution développée par la société ARUBA Network[22]. Il s'agit d'une solution de contrôle d'accès à proprement parler car elle couvre aussi bien les réseaux filaires, sans fils que les réseaux distants (VPN).

La solution offre la possibilité de développer, automatiser, appliquer et auditer une politique de sécurité des accès depuis une interface unique.

Le composant principal de la solution est un équipement (appliance) portant les technologies RADIUS et TACACS +. Le composant RADIUS sera utilisé pour authentifier les utilisateurs et le composant TACACS + sera lui utilisé pour authentifier les administrateurs lors de leurs activités d'exploitation. Autour de ces composants, viennent se greffer d'autres modules pour assurer entre autres les fonctionnalités de gestion de profil, création de rapports, intégration d'autres systèmes grâce à des API,… etc.

L'outil offre principalement différentes briques fonctionnelles :

- ✓ Traçabilité : nous avons la possibilité de suivre en temps réel un ensemble d'informations sur l'utilisateur (Nom de l'utilisateur, adresse MAC associée à sa machine, adresse IP utilisée par sa machine, système d'exploitation de sa machine[23], commutateur sur lequel il est connecté,…). L'utilisation de cette fonctionnalité devient efficiente lorsque nous sommes dans un environnement entièrement « Extrême Networks ».
- ✓ Contrôle d'accès : en utilisant le protocole 802.1x et l'authentification par adresse MAC.

[22] ARUBA Networks a été racheté par HP en mars 2015
[23] Le système d'exploitation utilisé sera identifié en analysant l'empreinte DHCP de la machine

- ✓ Accès invité : en utilisant un portail web pour l'accueil des invités, les utilisateurs invités pourront, soit se faire sponsoriser[24] pour un enregistrement par adresse MAC, soit utiliser un compte visiteur (login et mot de passe).
- ✓ Évaluation du client : qui est réalisée grâce au supplicant « On Guard ». Il vérifie les caractéristiques du poste de travail et impose qu'il soit conforme à une politique donnée avant d'autoriser l'accès au réseau.
- ✓ Double Authentification : la machine est authentifiée dans un premier temps grâce à un certificat ou son adresse MAC, puis, l'utilisateur est authentifié à son tour.
- ✓ SSO : L'utilisateur est automatiquement identifié lorsqu'il accède à son authentification après avoir passé l'authentification 802.1x.

7.2.2.3 NetSight

Netsight est un outil développé par la société Extrême Network. Il est avant tout un outil de gestion de réseau englobant un ensemble de fonctionnalités sur les réseaux filaires et sans fils tels que la supervision réseau, la gestion des configurations, ainsi que la génération de rapports.

En plus de toutes les fonctionnalités, il implémente également un module de contrôle d'accès au Réseau (NAC). Ce module est basé sur la technologie Free Radius. L'outil utilise donc les standards du marché ce qui lui permet de s'intégrer dans des environnements hétérogènes.

L'outil offre principalement quatre briques fonctionnelles :

- ✓ Traçabilité : nous avons la possibilité suivre en temps réel un ensemble d'informations sur l'utilisateur (Nom de l'utilisateur, adresse MAC associée à sa machine, adresse IP utilisée par sa machine, système d'exploitation de sa machine[25], commutateur sur lequel il est connecté,…).

[24] Envoi d'un email à une personne tierce appartenant à l'organisation pour validation
[25] Le système d'exploitation utilisé sera utilisé en analysant l'empreinte DHCP de la machine

L'utilisation de cette fonctionnalité devient efficiente lorsque nous sommes dans un environnement homogène « Extrême Networks ».

- ✓ Contrôle d'accès : en utilisant le protocole 802.1x et l'authentification par adresse MAC.
- ✓ Accès invité : en utilisant un portail web pour l'accueil des invités, les utilisateurs invités pourront soit se faire parrainer[26] pour un enregistrement par adresse MAC, soit utiliser un compte visiteur (login et mot de passe).
- ✓ Évaluation du client : qui peut être réalisée avec ou sans supplicant. L'ensemble des informations utilisées pour la fonctionnalité de traçabilité sont issues de cette brique. Pour le fonctionnement sans supplicant, l'outil va se baser sur un ensemble de logiciels, utilisés pour remonter des informations sur la machine déjà présentes sur le poste. Avec supplicant, il pourra s'agir du supplicant netsight ou encore de celui de Windows.

7.3 Avantages et inconvénients

Après avoir testé les solutions FreeRadius et Network Policy Server en maquette, il apparaît que :

Pour les solutions du libre, nous devons composer notre solution avec l'ensemble des briques fonctionnelles dont nous avons besoin. Dans le cadre de la mise en œuvre d'une politique globale de sécurité, la brique permettant le contrôle d'intégrité du poste utilisateur n'existe pas. En résumé, elles demandent beaucoup de temps pour développer et intégrer une solution de cette famille dans l'environnement de production.

Pour les solutions propriétaires, l'ensemble des briques ont été pensées. Elles proposent des fonctionnalités quasiment identiques. Elles intègrent toutes une brique permettant de contrôler l'intégrité du poste de l'utilisateur. La différence entre elles va se situer au niveau du protocole utilisé pour réaliser le contrôle

[26] Envoi d'un email à une personne tierce appartenant à l'organisation pour validation

d'intégrité[27] et de la philosophie de conception adoptée par le constructeur. Le choix d'une solution par rapport à une autre se fait donc en fonction de l'environnement dans lequel elle doit s'intégrer.

7.4 Solution adoptée

Actuellement le contrôle de l'accès au réseau est fait par domaine (accès distant, accès filaires, accès sans fils). Les solutions retenues dans chaque domaine sont différentes et liées à des marchés spécifiques. La démarche adoptée doit inclure l'optimisation des investissements réalisés. Nous avons donc choisi de faire converger les technologies existantes dans les domaines filaires et sans fils.

Comme évoqué dans la partie critères d'environnement, le contrôle de l'accès distant VPN est réalisé par la solution NETWORK CONNECT. Cette solution répond à des contraintes et à un besoin spécifique lié à ce périmètre.

Pour ce qui est du réseau sans fils, il est utilisé pour accéder au réseau intranet, donc à l'environnement de travail. Les équipes techniques disposent déjà d'une forte expérience sur les outils qui composent son infrastructure. Les utilisateurs sont également sensibilisés sur les manipulations du supplicant.

Le choix technique qui a été fait est de faire converger la gestion des deux réseaux. Ainsi, nous pourrons avoir une politique cohérente et renforcée en ce qui concerne l'accès au réseau interne. La technologie utilisée sera donc la solution JUNIPER UAC et son supplicant Odyssey.

[27] Les protocoles utilisés pour réaliser le contrôle d'intégrité des postes sont des solutions propriétaires.

Nous éliminons les solutions libres pour les raisons suivantes :

- elles demandent beaucoup de temps pour développer et intégrer une solution de cette famille dans l'environnement de production.
- Le développement de solutions « maisons » n'est pas dans la culture des équipes d'exploitation
- L'effort de documentation est non négligeable

Notre choix est d'implémenter une technologie propriétaire JUNIPER UAC car :

- Elles comportent l'ensemble des briques fonctionnelles liées à notre besoin
- Un support est assuré par les éditeurs.
- Il s'agit d'une technologie déjà utilisée sur l'infrastructure Wi-Fi.

7.5 Estimation du coût du projet

La solution est construite à partir d'une Appliance. Le prix public d'une Appliance de cette gamme est compris entre 3 000 € et plus de 300 000 € hors taxe selon le nombre d'utilisateurs (50 à 10 000) et les options retenues.

Les remises consenties par le fournisseur à ses grands comptes pouvant dépasser 50 %, il est difficile de donner un coût d'acquisition précis. Le coût de maintenance annuel est de l'ordre en général entre 8 % et 15 % du prix d'achat selon le client et les options du produit.

8 Déploiement de la solution adoptée

8.1 Planning de déploiement

La solution est déployée dans un premier temps sur le périmètre des équipes informatiques. Cela permettra aux équipes de s'approprier la nouvelle solution et de mieux appréhender les avantages et inconvénients de la technologie sans impacter les utilisateurs pendant la phase de mise au point. Ce déploiement sera une expérience grandeur réelle significative pour les futures extensions.

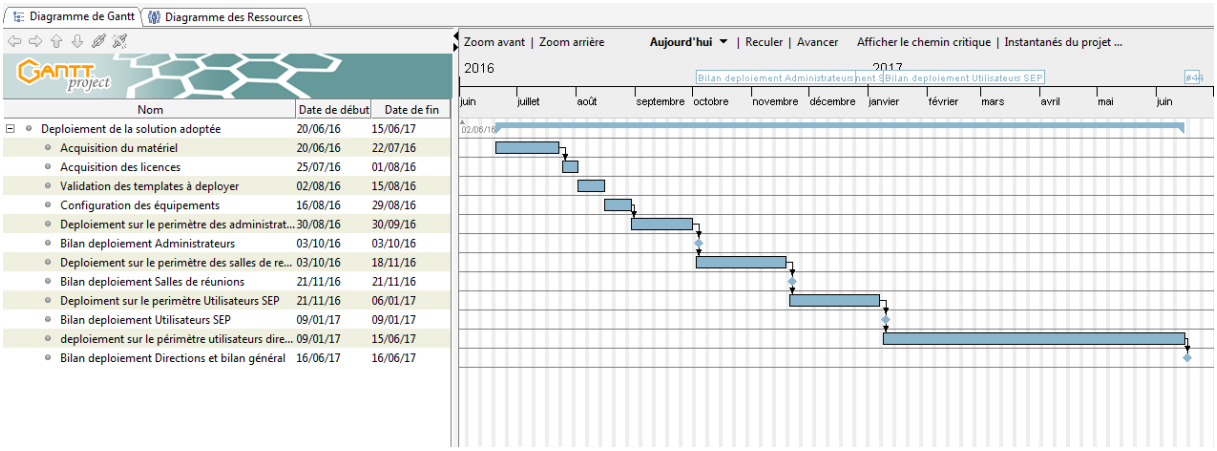


Figure 15 Planning de déploiement de la solution adoptée

Dans un second temps, nous allons nous intéresser au périmètre des salles de réunion où nous allons proposer, en plus de l'authentification 802.1x par supplicant, une authentification par enregistrement sur un portail web. Cette solution d'authentification sera utilisée pour les utilisateurs ne disposant pas de supplicant installé sur leur poste de travail. Ces derniers auront un accès limité aux ressources du réseau.

Enfin, nous activerons l'authentification des utilisateurs pour chacune des directions clientes au Secrétariat Général.

8.2 Architecture déployée

8.2.1 Présentation de la solution Juniper

Juniper propose une solution offrant un mécanisme d'authentification des utilisateurs et de contrôle d'intégrité des machines qu'ils utilisent lors de leur accès au réseau. Cette solution se nomme Juniper UAC (Unified Access Control) et est implémentée grâce à un Infranet Controler.

Elle permet d'offrir des accès au réseau en fonction d'exigences de sécurité conformes à une politique de sécurité définie. Ainsi, elle procure un service d'accès contrôlé à des utilisateurs non autorisés ou à des visiteurs.

On crée une politique de contrôle d'accès aux ressources. L'accès à ces ressources est basé sur la réussite du processus d'authentification.

Lors de son authentification, l'utilisateur est assigné à un rôle et une politique particulière de vérification de la conformité de sécurité de son poste. Par exemple nous allons pouvoir définir la version de l'antivirus nécessaire pour accéder au réseau (dernière signature antivirus).

La réussite de ce processus lui donne accès à un royaume portant les ressources auxquelles il souhaite accéder.

8.2.2 Intégration dans l'environnement

8.2.2.1 Architecture technique

L'ensemble des commutateurs sont affectés à des VLAN de la VRF d'administration. Ils ont donc une adresse IP appartenant à cette VRF. D'une manière générale, pour passer d'une VRF à une autre, il faut passer par un pare-feu. Les commutateurs d'étages ne portent qu'une seule adresse IP ; celle de leur interface d'administration.

Afin de sécuriser les échanges entre les différents éléments de l'authentification (point de contrôle et point de décision), nous allons donc placer notre point de décision dans la VRF d'administration.

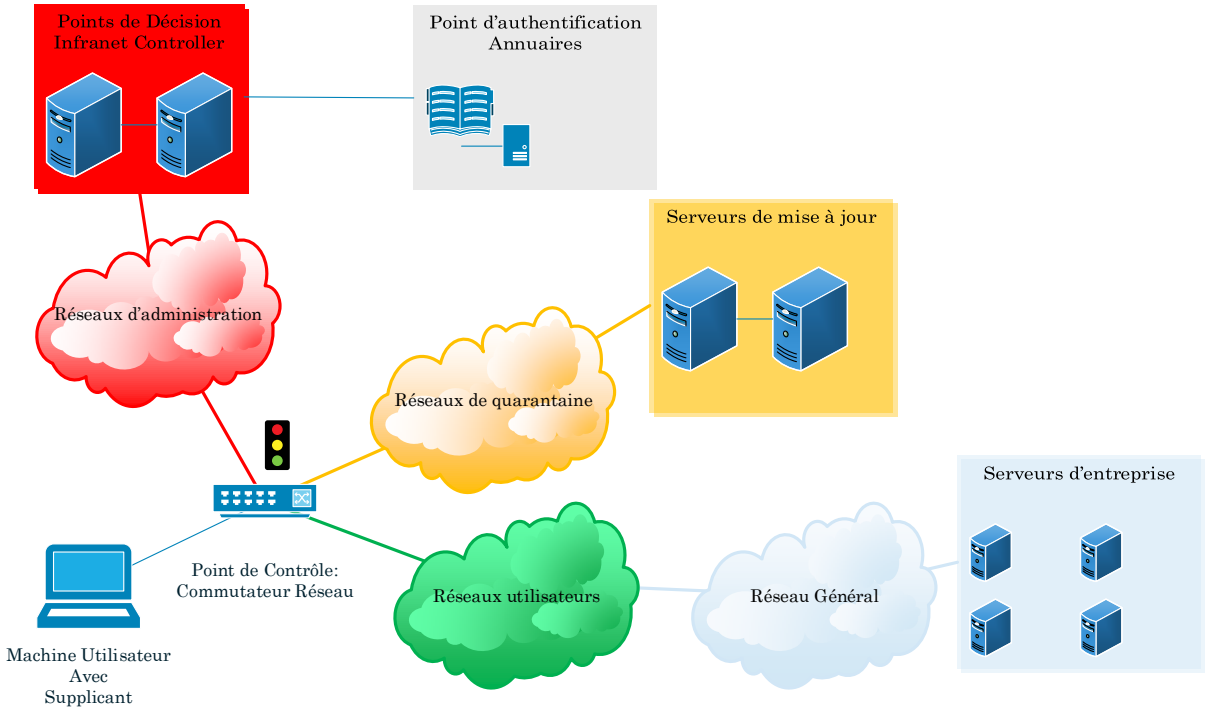


Figure 16 Intégration dans l'environnement du ministère

Pour la configuration, nous avons décidé d'utiliser les réseaux utilisateurs existants. Nous avons créé des réseaux de quarantaine par bâtiments. Dans ces réseaux de quarantaine, les utilisateurs auront accès à un ensemble de serveurs pour la réalisation des mises à jour.

8.2.2.2 Scénario d'authentification

Pour réaliser l'authentification et le contrôle d'intégrité, les commutateurs communiqueront avec les Infranet Controller à travers les réseaux d'administration représentés en rouge sur la figure 17 pour les différents échanges. Si la machine et l'utilisateur satisfont les critères d'authentification, le port du commutateur sera affecté au réseau de l'utilisateur représenté en vert sur la figure 17. En revanche si le poste de l'utilisateur ne répond pas aux exigences de sécurité, le port du commutateur sera affecté au réseau de quarantaine représenté en jaune sur la figure 17.

Si l'identité de l'utilisateur n'est pas reconnue, l'accès sera refusé.

8.2.2.3 Critères d'authentification :

La mise en place de solution de contrôle d'accès nous emmène à nous concentrer sur les utilisateurs et leurs usages. Nous allons donc définir des profils d'utilisateurs auxquels nous associerons des méthodes d'authentification.

Dans le périmètre du secrétariat général, nous retrouvons trois grandes familles de populations : les agents du ministère, les administrateurs du système d'information (SI) dont je fais partie et les visiteurs du ministère. À chaque famille va correspondre une spécificité d'identification.

Identification de l'utilisateur	Authentification	Paramètres du poste utilisateur			Accès au réseau dedié	
		Poste du SG	Antivirus actif	Antivirus à jour	Bureau	Salle de réunion
Agents du ministère - login/mdp	✔	✔	✔	✔	Utilisateurs	Utilisateurs
	✔	✔	✔	✖	Quarantaine	Quarantaine
	✔	✔	✖	N/A	Quarantaine	Quarantaine
	✖	N/A	N/A	N/A	Refusé	Refusé
Administrateurs SI - certificat	✔	✔	✔	✔	Administrateurs	N/A
	✔	✔	✖	N/A	Quarantaine	N/A
	✔	✔	✔	✖	Quarantaine	N/A
	✖	N/A	N/A	N/A	Refusé	Refusé
Autres - portail visiteur	✔	✖	N/A	N/A	Refusé	Visiteurs
	✖	N/A	N/A	N/A	Refusé	Refusé

Tableau 4 Définition des critères d'authentification

Dans tous les cas non définis ci-dessus, l'accès au réseau sera refusé.

8.2.3 Configuration des commutateurs

Les commutateurs d'étages utilisés dans l'infrastructure du ministère sont de marque 3Com, H3C et HP. La gamme des équipements de ces constructeurs est similaire, il s'agit de la gamme 5500. Nous allons définir un modèle unique de configuration qui sera installé sur l'ensemble des équipements.

Le standard 802.1x apporte une flexibilité hors du commun pour le contrôle d'accès. Nous allons pouvoir déterminer, sur un port donné du commutateur, la stratégie à adopter lorsqu'un équipement est branché, le nombre de sessions différentes autorisées[28],….

8.2.3.1 Configuration de base du commutateur

Nous allons donc retrouver sur l'ensemble des équipements une configuration de base. Le premier élément de configuration est un processus définissant les paramètres nécessaires au commutateur (point de contrôle) pour dialoguer avec le serveur d'authentification (point de décision).

```
[Switch] radius scheme radius1
[Switch-radius-radius1] primary authentication X.X.X.X 1812 key abcdefg
[Switch-radius-radius1] user-name-format without-domain
[Switch-radius-radius1] nas-ip Y.Y.Y.Y
[Switch-radius-radius1] quit
```

Table 1 Déclaration du serveur RADIUS

On définit le nom du processus « radius1 », l'adresse IP du serveur d'authentification « X.X.X.X[29] » accompagnée du port sur lequel il va écouter et du mot de passe partagé « abcdefg », le format attendu du nom d'utilisateur,

[28] En général, dans les zones où la téléphonie sur IP est déployée, on mutualise le câblage entre la téléphonie et l'usage bureautique. Ainsi le poste téléphonique et le poste utilisateur partagent le même câble physique et donc le même port du commutateur.
[29] L'adresse IP du serveur d'authentification sera l'adresse virtuelle partagée par les deux nœuds de notre cluster actif / passif.

l'adresse IP à utiliser par le commutateur « Y.Y.Y.Y » pour dialoguer avec le serveur.

Le second élément de la configuration de base est le domaine. Dans ce domaine nous allons définir les politiques d'authentification et d'autorisation en les associant au processus radius que nous avons précédemment défini.

```
[Switch] domain auth_radius
[Switch-isp-auth_radius] authentication lan-access radius-scheme radius1
[Switch-isp-auth_radius] authorization lan-access radius-scheme radius1
[Switch-isp-auth_radius] quit
[Switch] domain default enable auth_radius
```

Table 2 Déclaration des politiques d'authentification et d'autorisations

On retrouve le nom du domaine « auth_radius » ; la politique à appliquer en cas de demande d'accès au réseau « lan-access radius-scheme radius1 » pour l'authentification et celle à appliquer en cas de demande d'accès au réseau « lan-access radius-scheme radius1 » pour l'autorisation d'accès. Enfin, on active le domaine en le paramétrant par défaut. Lorsqu'un utilisateur ne spécifiera pas de domaine, il sera automatiquement rattaché à ce domaine et la politique que nous venons de spécifier s'appliquera si l'authentification est activée sur le port sur lequel il est connecté.

Ainsi, lorsqu'un utilisateur se connectera sur un port où l'authentification 802.1x est activée, le commutateur va l'affecter au domaine « auth_radius ». Dans ce domaine, il est défini que pour s'authentifier, on doit utiliser le processus radius1. Le commutateur va donc utiliser le mot de passe partagé avec le serveur d'authentification pour se faire approuver, puis il va s'appuyer sur ce dernier pour réaliser l'authentification.

Le mode d'authentification 802.1x doit être configuré sur l'interface physique du commutateur pour que l'ensemble du processus d'authentification se déclenche. Cette configuration peut être granulaire en fonction des éléments que nous retrouvons dans son environnement.

8.2.3.2 Configuration spécifique en fonction de l'environnement utilisateur

Pour configurer le mode d'authentification 802.1x sur un port, nous devons connaître l'environnement utilisateur. En effet, un utilisateur utilisant un poste IP, doit pouvoir être joignable au téléphone, même s'il n'arrive pas à s'authentifier.

Dans l'illustration ci-après, nous retrouvons :

- ✓ Le port du commutateur en mode « Hybrid » ainsi, nous pouvons y connecter un téléphone IP et un poste utilisateur (port link-type hybrid).
- ✓ Le vlan dédié à la voix. Les paquets à destination de ce vlan sont tagués [30](port hybrid vlan 53 tagged ; voice vlan 53 enable).
- ✓ Le vlan à utiliser par défaut[31]. Ce vlan sera celui dédié au poste utilisateur.
- ✓ Nous activons également la technologie POE[32] qui permet au téléphone de s'alimenter électriquement sur le commutateur à travers le réseau de câblage (poe enable).

Tous ces éléments sont ceux que nous retrouvons de base sur les commutateurs.

```
port link-mode bridge
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 53 tagged
voice vlan 53 enable
port hybrid vlan 382 untagged
port hybrid pvid vlan 382
poe enable
undo dot1x handshake
dot1x critical vlan 382
```

[30] Le tagguage est un marquage du paquet IP.
[31] En cas de non marquage des paquets IP
[32] Power Over Ethernet est la technologie qui permet de délivrer l'alimentation électrique d'équipement à travers un câble Ethernet en même temps que la transmission des données.

```
dot1x
```

Table 3 Configuration du port d'un commutateur accueillant un téléphone IP

Pour la partie authentification 802.1x, nous allons retrouver :

- ✓ La désactivation du handshake[33] (undo dot1x handshake)
- ✓ La définition du vlan critique (dot1x critical vlan 382) ; il s'agit du réseau dans lequel l'utilisateur sera autorisé à se connecter par défaut en cas de défaillance générale des points de décision.
- ✓ L'activation du protocole 802.1x sur le port (dot1x).

Pour un utilisateur n'ayant pas de poste IP, mais plutôt un poste téléphonique classique, nous retrouvons dans l'illustration ci-après la configuration du port du commutateur.

```
port link-mode bridge
port access vlan 382
undo dot1x handshake
dot1x critical vlan 382
dot1x
```

Table 4 Configuration du port d'un commutateur n'accueillant pas un téléphone IP

Dans sa configuration de base, le port sera affecté à un vlan par défaut. Nous retrouvons :

- ✓ La désactivation du handshake (undo dot1x handshake)
- ✓ La définition du vlan critique (dot1x critical vlan 382) ; il s'agit du réseau dans lequel l'utilisateur sera autorisé à se connecter par défaut en cas de défaillance générale des points de décision.

Pour les salles de réunion, on retrouvera la même configuration que celle d'un utilisateur n'ayant pas de téléphone IP. À cette configuration, nous allons spécifier le vlan dédié aux visiteurs. Ainsi lorsqu'un visiteur du ministère des finances se connecte sur une prise réseau en salle de réunion, le commutateur va

[33] Le handshake est un mécanisme périodique de vérification de la présence de l'utilisateur. Cette fonctionnalité est mal supportée par les systèmes Windows.

détecter qu'il n'est pas compatible avec le protocole 802.1x. Il va donc le rediriger automatiquement vers un réseau visiteur. Depuis ce réseau visiteur, il aura uniquement accès à internet.

```
port link-mode bridge
port access vlan 382
undo dot1x handshake
dot1x critical vlan 382
dot1x guest-vlan 300
dot1x
```

Table 5 Configuration du port d'un commutateur en salle de réunion

8.2.4 Configuration du point de décision

Nous avons acquis deux équipements de marque Juniper et de type UAC. L'administration de ces équipements se fait par l'interface web. Pour la haute disponibilité, un de ces équipements est installé sur le site principal et le second l'est sur le site de secours. Le mode de fonctionnement que nous avons choisi est le mode actif/passif.

Avec le mode actif / passif, nous allons avoir un équipement « maître » qui porte une adresse IP virtuelle pour recevoir les requêtes des utilisateurs. Le second sera « l'esclave ». Il pourra prendre le relais en cas de défaillance du premier.

On configure le système de haute disponibilité sur les équipements en ajoutant un nœud esclave comme membre autorisé depuis le nœud maître, avec un nom, une adresse IP et un mot de passe partagé qui sera demandé à tout équipement souhaitant rejoindre le cluster.

Ensuite, on réitère la même opération depuis le nœud esclave pour déclarer le nœud maître.

8.2.4.1 Définition de la politique de conformité du poste

Pour vérifier la conformité du poste de l'utilisateur, on utilise un « host checker ». Il permet de faire des vérifications de sécurité sur le poste client. Par exemple, on

peut vérifier que certains processus ou encore certaines applications sont activés sur le poste avant d'autoriser l'accès aux ressources. Si l'utilisateur n'est pas conforme à la politique de sécurité, on peut lui renvoyer un ensemble d'instructions lui permettant de se conformer aux exigences de sécurité.

Concrètement on peut par exemple vérifier la présence d'un antivirus en particulier, d'un pare-feu, ou encore d'un antimalware, antispyware et même l'OS utiliser.

Figure 17 Règle de conformités du poste aux exigences de la politique de sécurité

Nous avons défini trois règles :

- ✓ La présence d'un antivirus activé sur le poste,
- ✓ La vérification des dernières signatures antivirales datant de moins de 5 jours
- ✓ L'appartenance du poste de l'utilisateur au parc des MEF

Pour vérifier la présence de l'antivirus sur le poste, le supplicant va s'assurer que le processus « ccSvcHst.exe » est actif.

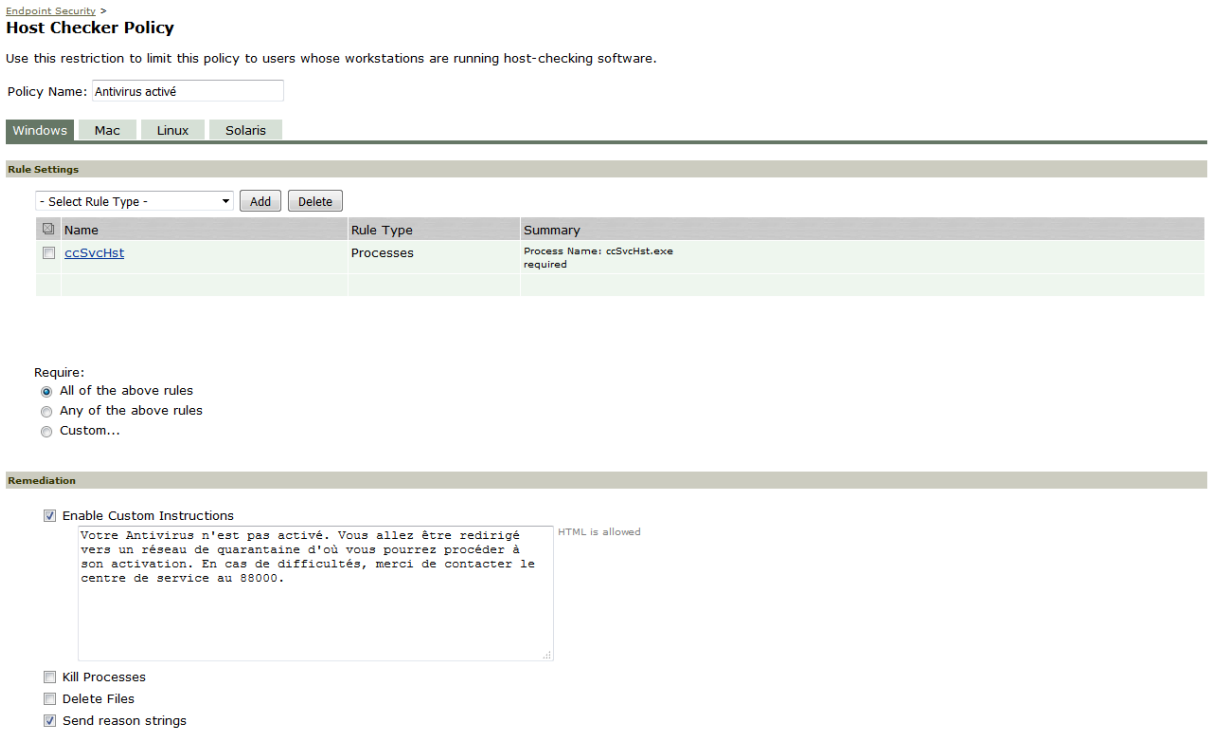


Figure 18 Vérification du processus antivirus activé

L'utilisateur est informé qu'il est redirigé vers une zone de quarantaine si son antivirus n'est pas activé.

Après avoir vérifié que l'antivirus est bien actif sur le poste de l'utilisateur, nous nous assurons qu'il est à jour. Pour cela, nous définissons, dans une règle, les versions des antivirus utilisés et nous demandons à l'infranet controller de vérifier que la version installée sur le poste est à jour avec une tolérance de cinq jours.

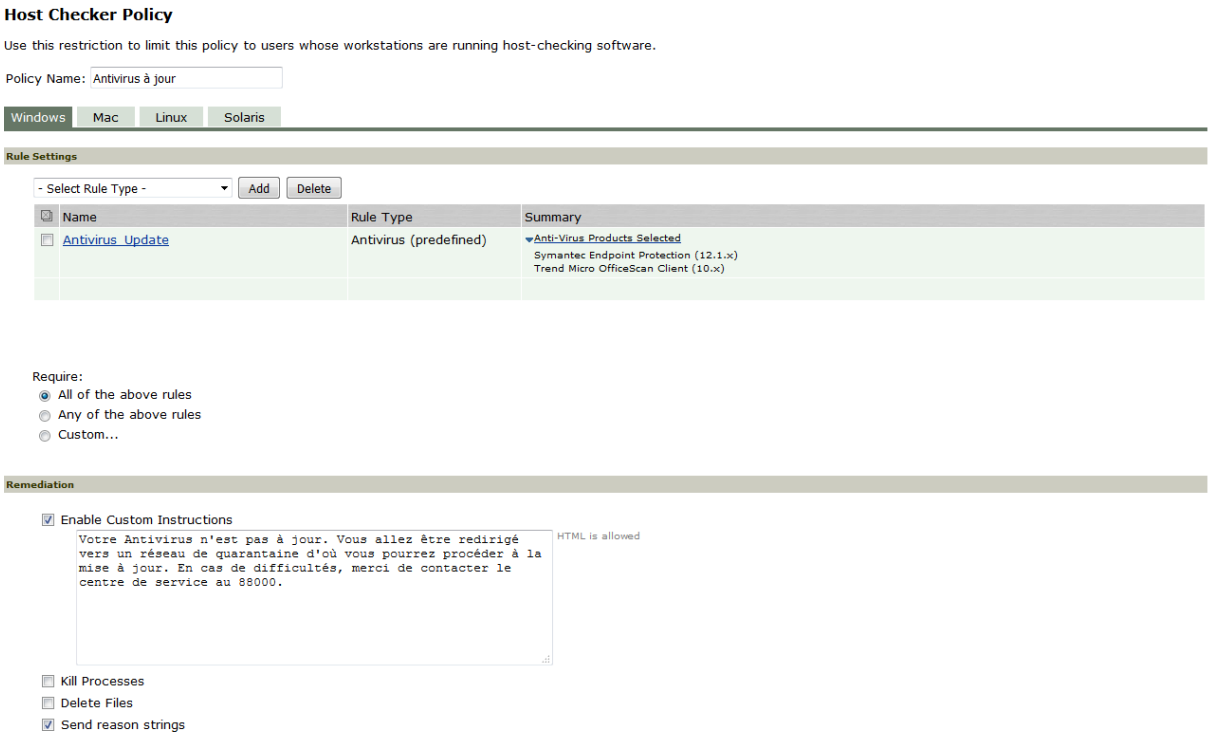


Figure 19 Vérification des signatures de l'antivirus

Nous retrouvons ci-après la règle permettant de définir les antivirus utilisés pour le parc.

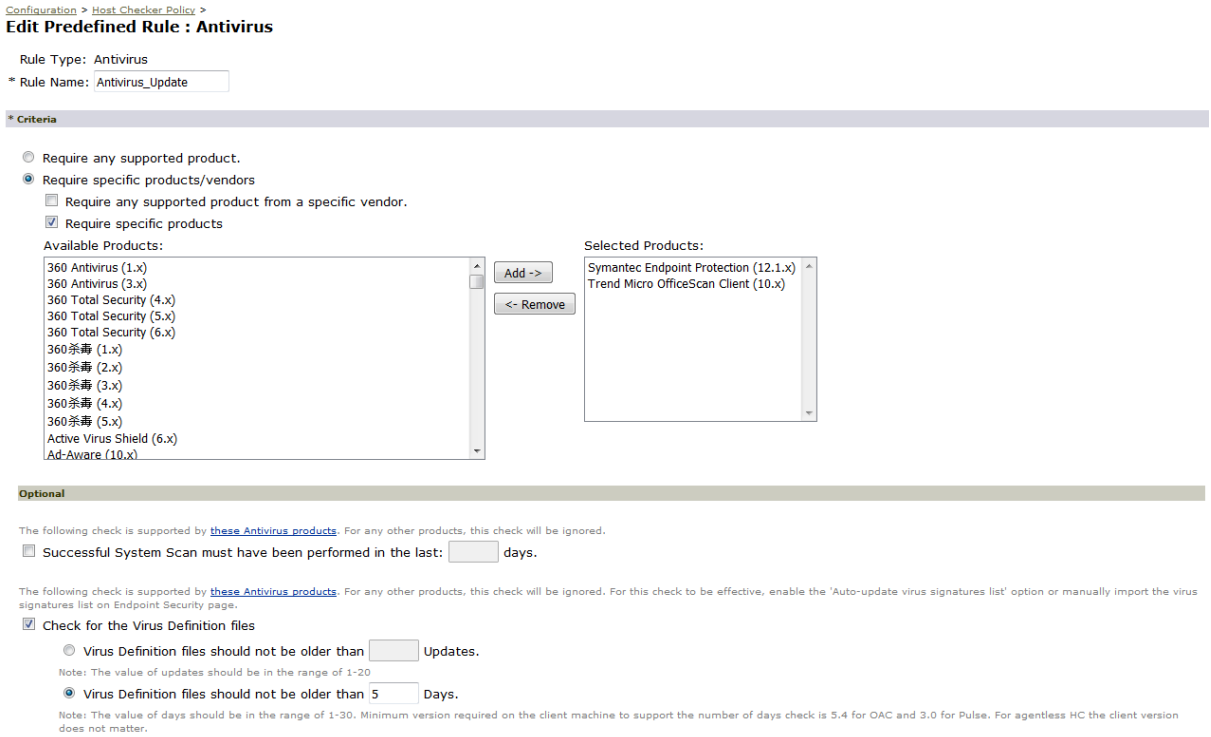


Figure 20 Définition de la version de l'antivirus

En ce qui concerne l'appartenance du poste au parc du ministère, nous allons vérifier un paramètre spécifique porté par l'ensemble des postes du ministère.

8.2.4.2 Définition des serveurs d'authentification

Pour authentifier les utilisateurs, l'Infranet Controller va se reposer sur un annuaire. Nous devons le paramétrer afin qu'il puisse l'interroger. Dans ce paramétrage, on retrouve :

- ✓ L'adresse IP de l'annuaire,
- ✓ Le port sur lequel l'interrogation doit se faire,
- ✓ Le type de serveur LDAP, le mode de connexion,
- ✓ Les paramètres requis pour que l'Infranet controller s'authentifie auprès de l'annuaire.

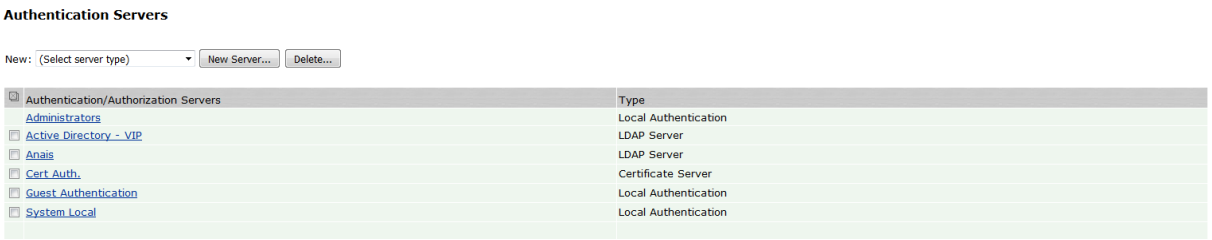


Figure 21 Déclaration des serveurs d'authentification

Nous nous reposons sur trois serveurs :

- ✓ Active Directory – VIP : l'annuaire active directory dans lequel sont renseignés tous les utilisateurs du secrétariat général.
- ✓ Anais : l'annuaire LDAP centralisé du ministère dans lequel on retrouve les utilisateurs de l'ensemble des directions du ministère[34].
- ✓ Certh Auth : Le serveur permettant de vérifier la non-révocation du certificat présenté par l'utilisateur.

Lorsque l'utilisateur s'authentifiera par certificat, le champ « CN » du certificat sera extrait pour être vérifié dans l'annuaire.

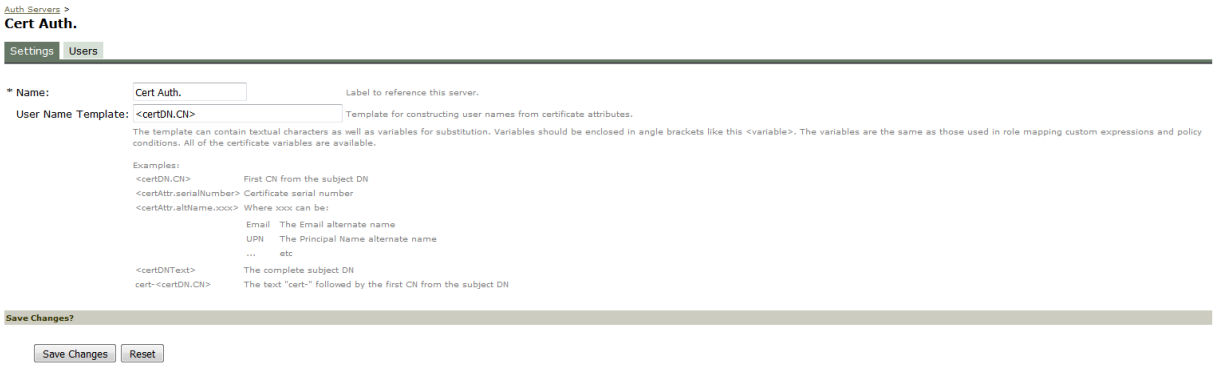


Figure 22 Extraction du champ du certificat pour vérification

Une fois le champ « CN » du certificat extrait, l'Infranet controller va vérifier sur la liste des certificats révoqués que le certificat est toujours valide. Ensuite, il va vérifier dans l'annuaire que l'utilisateur existe et en fonction des paramètres des royaumes ou des rôles, il va autoriser l'utilisateur à se connecter.

[34] Cet annuaire est renseigné en anticipation de l'ouverture du service d'authentification aux directions composant le ministère.

8.2.4.3 Définition de la stratégie d'accès des utilisateurs

L'accès des utilisateurs aux royaumes se fait à travers une URL. Cette URL est le point d'entrée unique auquel est associée une page de login non vue par l'utilisateur du fait de l'utilisation du supplicant Odyssey.

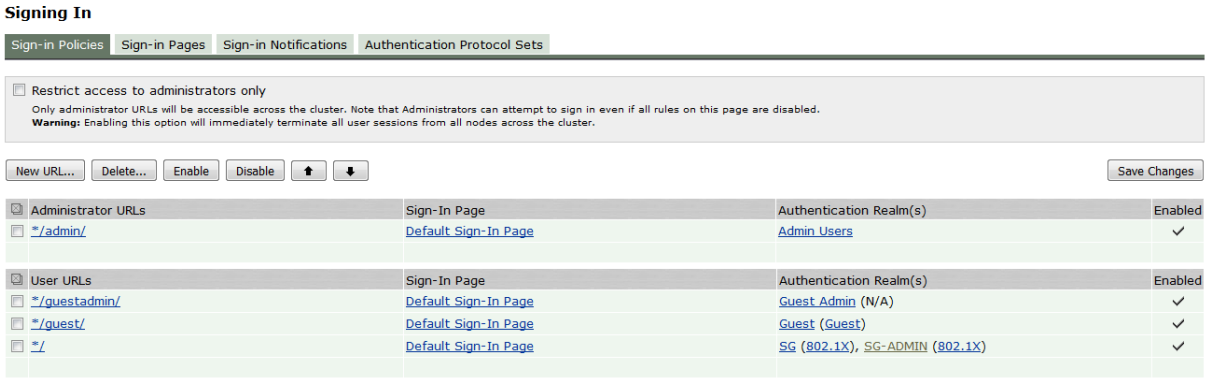


Figure 23 URL d'accès aux royaumes

Comme nous le constatons dans la figure ci-après, à chaque fois qu'on associe un royaume à l'URL, nous devons spécifier le protocole d'authentification associé au royaume.

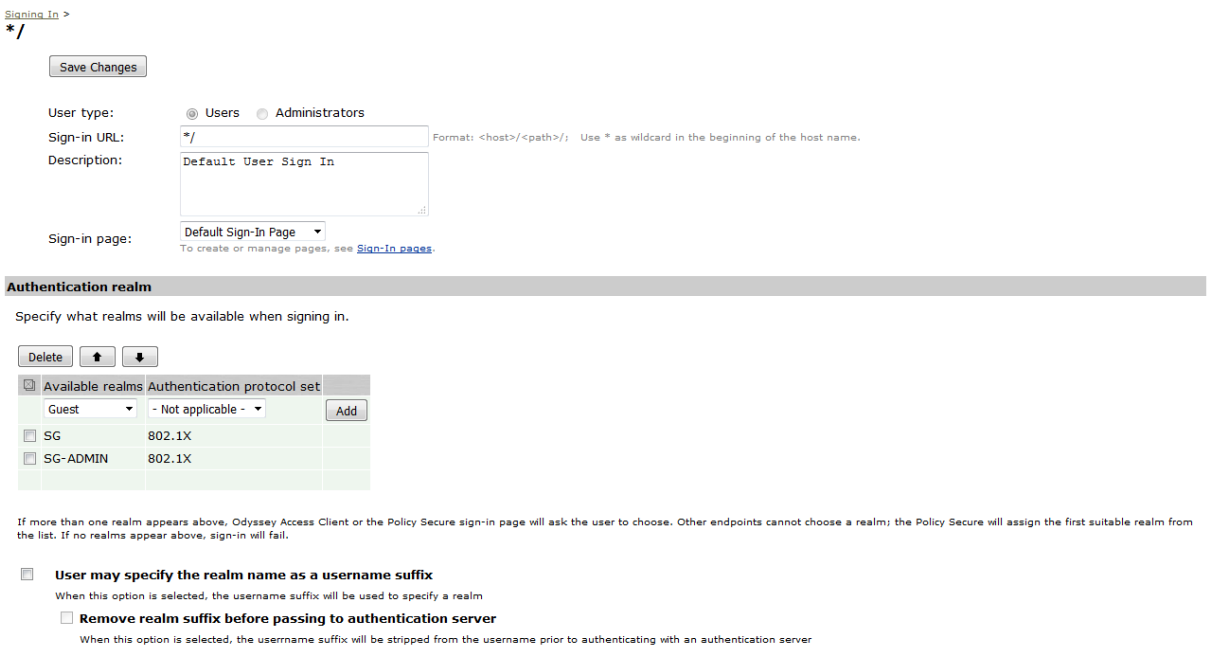


Figure 24 Association de l'URL aux royaumes

8.2.4.4 Définition des Royaumes d'authentification

Les royaumes d'authentification permettent aux utilisateurs de s'authentifier. Ils contiennent des politiques indiquant dans quelles conditions l'utilisateur est autorisé à accéder au système. Par exemple, on peut autoriser un accès uniquement si l'utilisateur se connecte d'un emplacement spécifique. L'appartenance à un royaume est déterminée en fonction de l'identité de l'utilisateur, du serveur d'authentification définit et du mode d'authentification utilisé. On associe un royaume à un mode d'authentification donné en configurant la stratégie d'accès.

Le royaume d'authentification est composé de l'ensemble des éléments permettant l'authentification de l'utilisateur. On y retrouve :

- ✓ Le serveur d'authentification : L'infranet controller va lui transmettre les informations de l'utilisateur qu'il a reçu afin de vérifier son identité.
- ✓ La politique d'authentification : indique les éléments de sécurité requis avant qu'un l'Infranet controller ne sollicite le serveur d'authentification.
- ✓ L'affectation aux rôles : spécifie les critères nécessaires à un utilisateur pour être affecté à un rôle.

Figure 25 Royaumes d'authentification définis

Dans notre cas, nous avons défini deux royaumes différents : « SG » et « SG-ADMIN ».

Le royaume « SG » : est celui dédié aux agents du ministère.

Pour accéder à ce royaume, l'identité de l'utilisateur sera vérifiée auprès de l'annuaire Active Directory que nous avons défini plus haut. Son profil utilisateur sera également vérifié auprès de ce même annuaire.

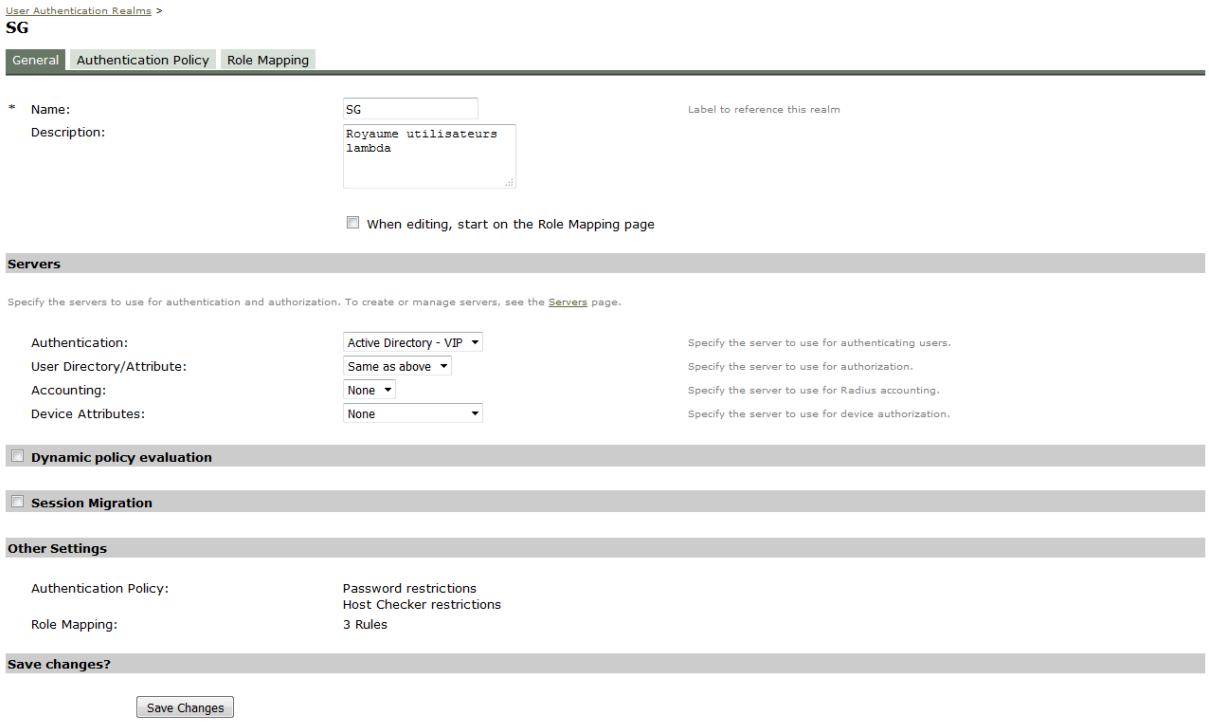


Figure 26 Royaume SG - Définition d'ensemble

Également, son poste doit être conforme à la politique de sécurité du ministère ainsi, nous évaluons à l'entrée du royaume les paramètres définis par la politique de sécurité. Ce sont ces paramètres qui seront les conditions d'accès aux différents rôles.

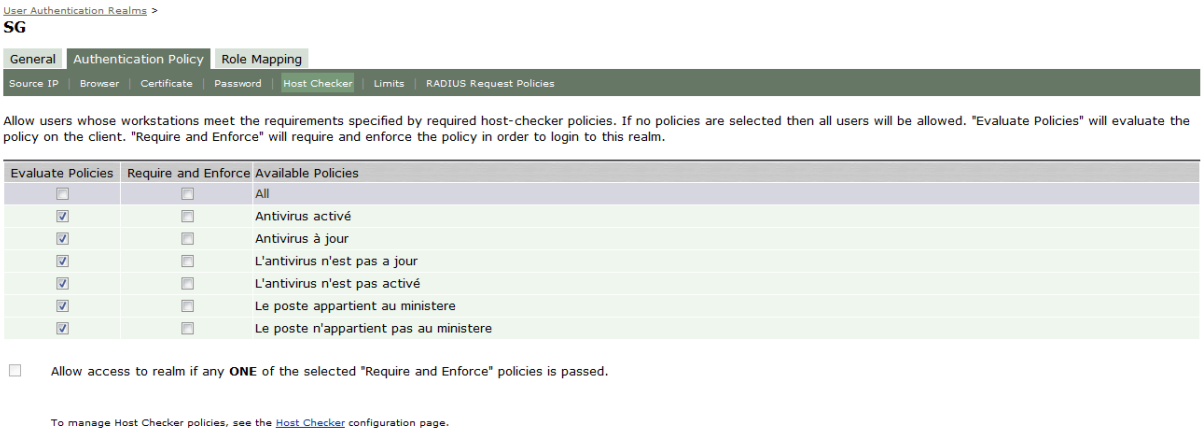


Figure 27 Royaume SG - Evaluation de la politique de conformité du poste utilisateur

Un utilisateur de royaume SG peut se voir attribué en fonction de l'état de son poste utilisateur trois rôles : Le rôle « Quarantaine », « GUEST-SG » ou encore « USER-SG ».

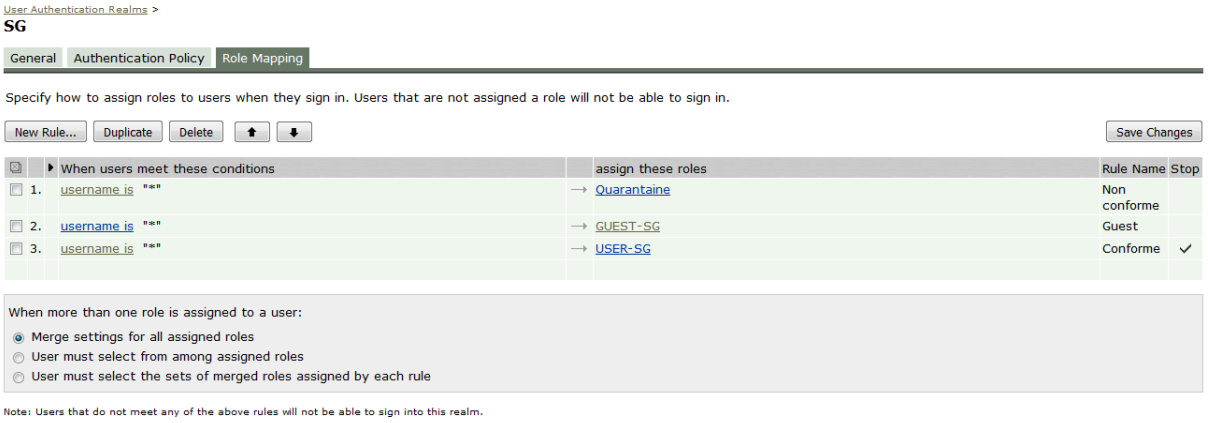


Figure 28 Royaume SG - Affectation des rôles

Nous voyons un peu plus loin comment est interprétée l'attribution de ce rôle.

Pour ce qui est du royaume « SG-ADMIN », on exige un certificat utilisateur pour se connecter. Ce certificat est vérifié dans l'annuaire « anais » que nous avons défini plus haut. La politique de conformité du poste est identique à celle du royaume « SG ».

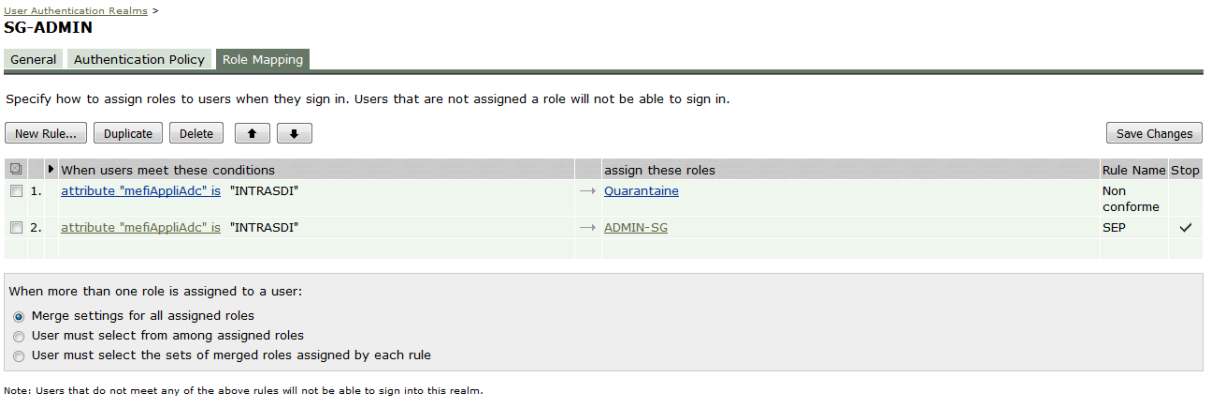


Figure 29 Royaume SG-ADMIN - Affectation des rôles

Pour ce royaume, nous sommes plus exigeants que pour les autres. Un champ spécifique de l'annuaire sera vérifié afin de s'assurer que l'utilisateur appartient bien aux équipes techniques informatiques du ministère. Le cas échéant il sera rejeté.

Dans le cas où le poste utilisateur n'est pas à jour, il se voit automatiquement attribuer le rôle « Quarantaine ».

8.2.4.5 Définition des rôles utilisateurs

Les rôles définissent les paramètres de session de l'utilisateur. À ce niveau, on définit la manière dont l'utilisateur se connecte[35]. On peut spécifier des conditions d'accès aux ressources en fonction de l'adresse IP attribuée aux utilisateurs, ou encore exiger un certificat pour y accéder. Également, on pourra exiger des éléments de conformité du poste. Le fait d'appartenir à un rôle ou un autre est défini par les attributs radius que nous allons collecter.

[35] Un utilisateur peut avoir sur sa machine le supplicant ou il peut le télécharger au moment de la connexion

Figure 30 Définition des rôles utilisateurs

Dans notre cas nous avons défini quatre rôles différents :

- ✓ ADMIN-SG : dédié aux administrateurs SI, il sera restreint aux utilisateurs ayant un certificat déclaré dans le rôle. Les postes utilisateurs auront un supplicant installé et on vérifiera la conformité du poste.
- ✓ USER-SG : dédié aux utilisateurs (agents du ministère) dont les postes répondent à la politique de conformité définie par la politique de sécurité.
- ✓ Quarantaine : dédié aux utilisateurs (agents du ministère) dont les postes ne répondent pas à la politique de conformité[36] définie par la politique de sécurité.
- ✓ GUEST-SG : dédié aux visiteurs du secrétariat général, la condition d'accès à ce rôle sera que le poste utilisé n'appartienne pas au ministère des finances.

8.2.4.6 Définition des clients RADIUS (Équipement de connexions)

Pour que les commutateurs puissent échanger des informations avec leur point de décision, il faut qu'ils soient déclarés sur l'Infranet Controller.

Pour cela, on va les répartir en groupes logiques : « location group ». À ces groupes logiques, nous allons associer l'URL utilisée pour l'accès des utilisateurs.

[36] Nous retrouvons dans les pages suivantes les éléments retenus pour la vérification de conformité du poste utilisateur.

On ne peut associer qu'une seule URL par « location group ». Ainsi le « location group » associe la stratégie d'accès de l'utilisateur au commutateur.

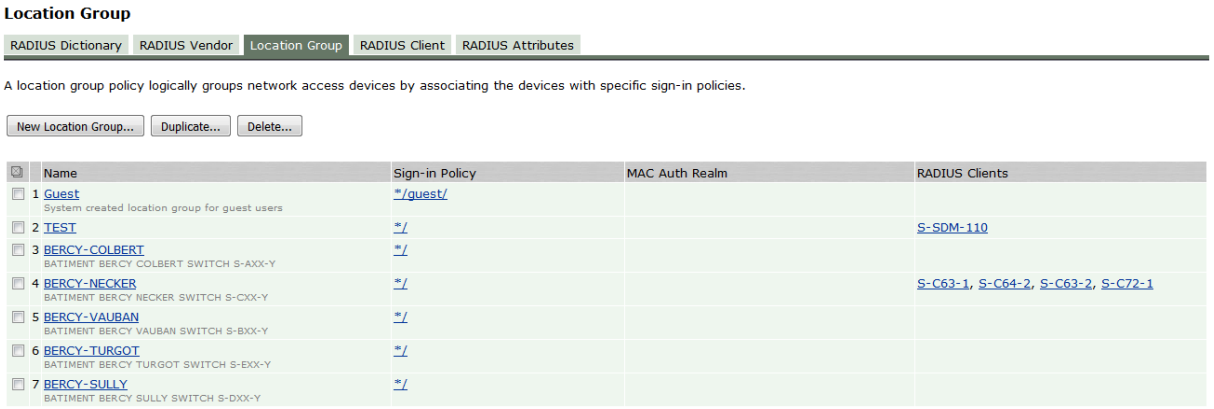


Figure 31 Définition des "location group"

Une fois les « location group » créés, nous allons pouvoir leur associer des commutateurs dans l'onglet RADIUS Client. Nous allons donc renseigner :

- ✓ L'adresse IP du commutateur,
- ✓ Le mot de passe RADIUS partagé entre le commutateur et l'Infranet Controller,
- ✓ Le modèle du commutateur,
- ✓ Le location group associé.

Pour configurer l'Infranet Controller comme un serveur RADIUS pour 802.1x, on doit configurer un 'location group", une "RADIUS access policy" et des "RADIUS attributes".

Pour associer un rôle utilisateur à une action du commutateur, nous allons utiliser les attributs RADIUS dans l'onglet « RADIUS Attributes ».

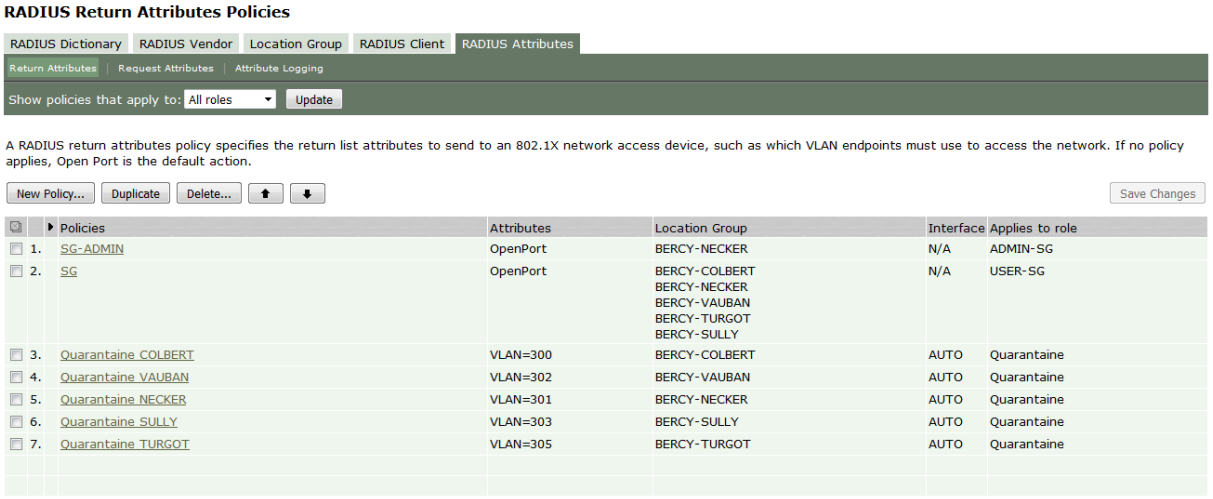


Figure 32 Association du rôle de l'utilisateur à une action du commutateur

Dans la figure ci-dessus, nous indiquons la stratégie à adopter en fonction du rôle attribué à l'utilisateur et de l'emplacement de sa connexion.

Concrètement, si un utilisateur est affecté au rôle « Quarantaine », le port du commutateur sur lequel il est connecté sera automatiquement affecté, en fonction de l'endroit où il se connecte, à l'un des vlan de quarantaine que nous avons indiqués. En revanche, s'il est affecté à un des rôles « ADMIN-SG » ou « USER-SG », son accès sera autorisé sur le vlan préprogrammé sur le port.

L'Infranet Controller va, en fonction du rôle attribué à l'utilisateur, vérifier dans l'ordre qu'il correspond à l'une des règles énoncées dans la figure ci-dessus.

Après avoir configuré l'Infranet Controller, nous pouvons procéder à la configuration des postes utilisateurs.

8.2.5 Configuration du poste utilisateur

Sur le poste de l'utilisateur, nous allons installer un agent logiciel : le supplicant. La solution Juniper propose son propre supplicant « Odyssey ». Cet agent supporte les différents modes d'authentification 802.1x et utilise le protocole propriétaire « EAP – JUAC » pour le contrôle d'intégrité.

Il va permettre de récupérer les informations nécessaires pour l'authentification de l'utilisateur, la vérification de la conformité du poste utilisateur aux exigences

de la politique de sécurité définie pour les communiquer au point de décision par l'intermédiaire du commutateur.

Les agents du ministère et les administrateurs SI n'ayant pas le même mode d'authentification, nous allons générer des profils de connexion propres à chacun d'eux. Ces profils seront télé distribués et configurés à distance sur les machines des utilisateurs en même temps que les mises à jour habituelles avant l'activation de la solution.

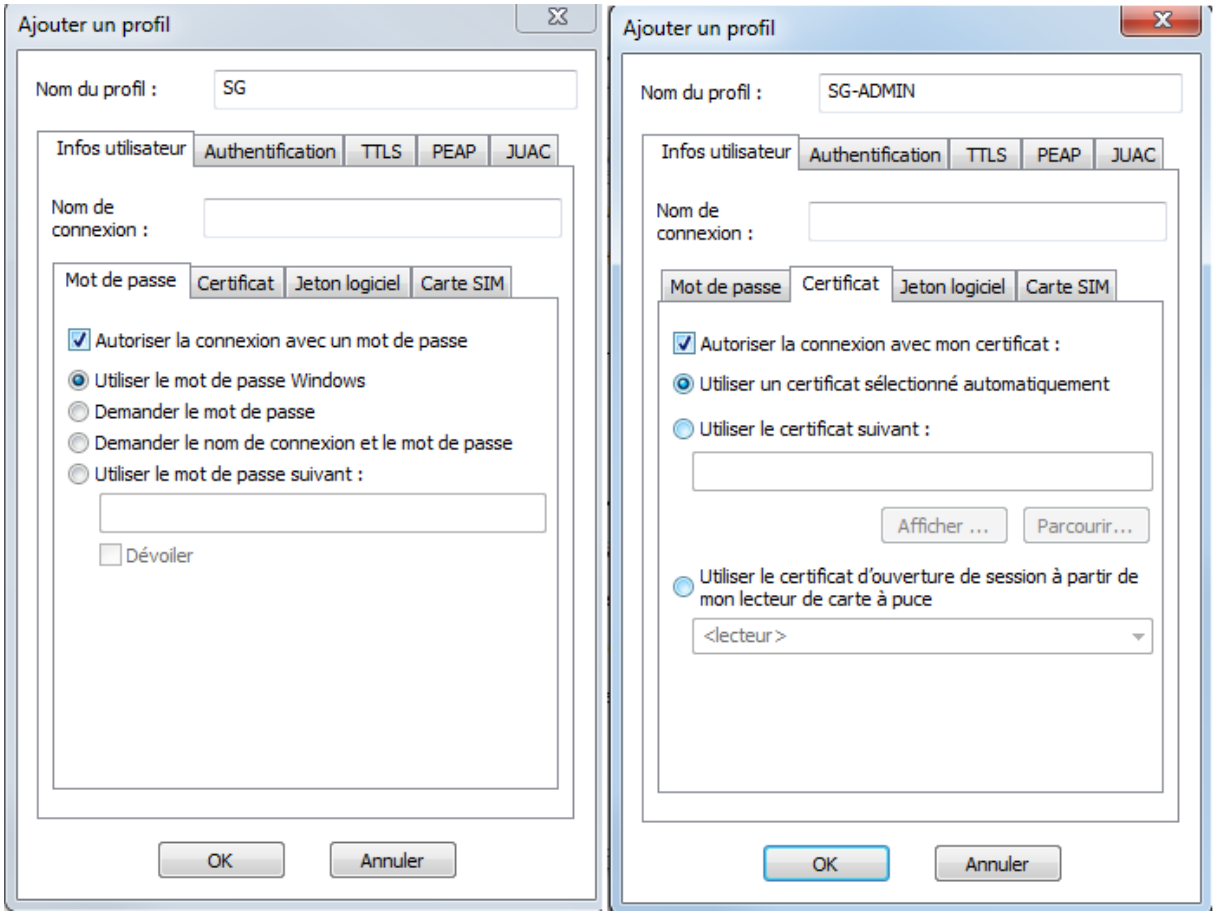


Figure 33 Création des profils de connexion

Dans la figure ci-dessus, nous créons les profils correspondants aux royaumes définis :

- ✓ Dans l'onglet « Authentification », nous indiquons le protocole utilisé pour réaliser l'authentification de l'utilisateur. Dans notre cas ce sera EAP TTLS.

- ✓ Puis, nous allons spécifier dans l'onglet « TTLS », le protocole qui va être utilisé entre le supplicant et l'Infranet Controller. Dans notre cas ce sera EAP – JUAC.
- ✓ Enfin, nous allons indiquer à quel royaume le profil défini correspond dans l'onglet JUAC comme présenté dans la figure ci-après.

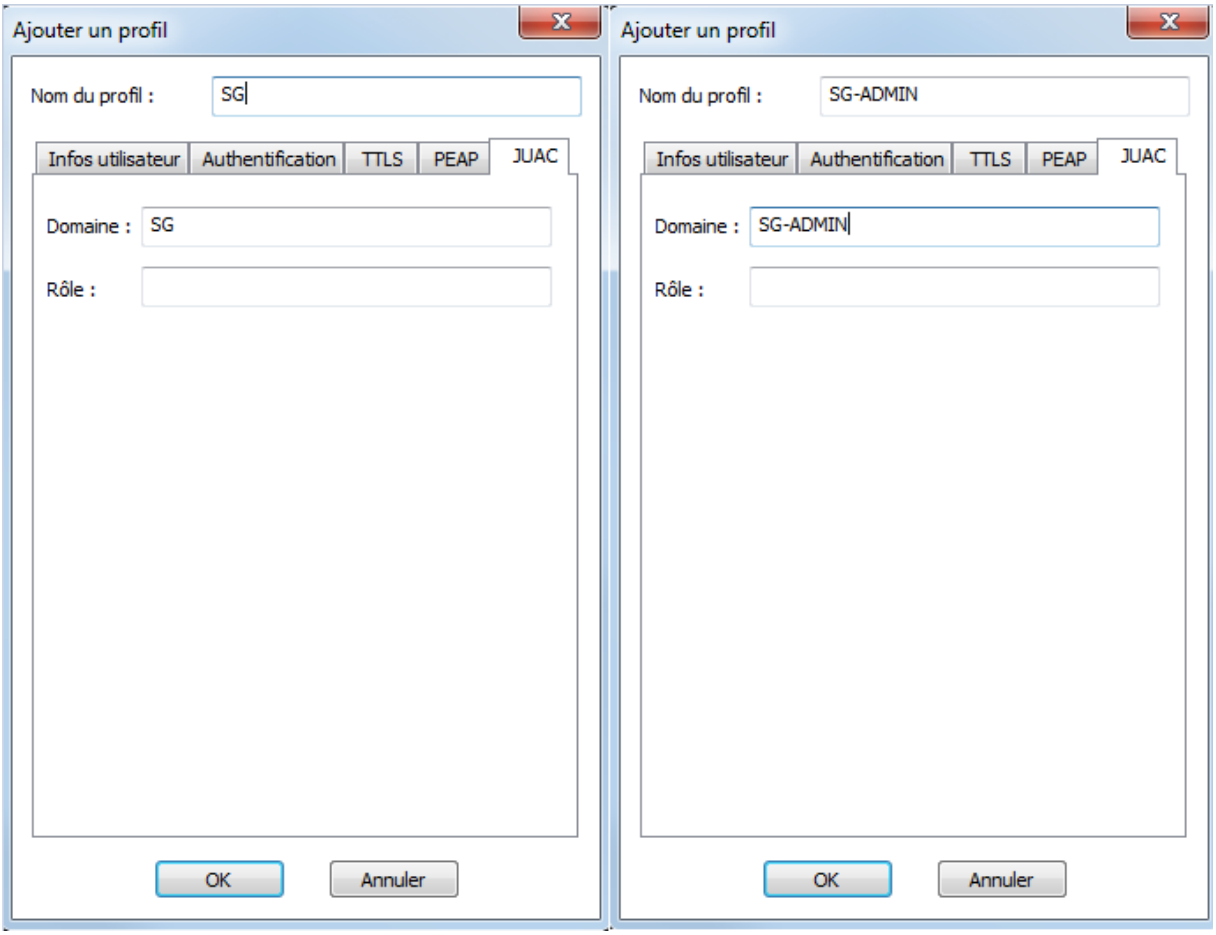


Figure 34 Association des royaumes aux profils de connexions

Ainsi, lors de la première requête de l'utilisateur, le supplicant va automatiquement spécifier le royaume auquel il souhaite accéder. Le mode d'authentification choisi en fonction de son profil correspond à la stratégie d'accès définie au niveau du royaume.

Le contrôleur Juniper UAC est en mode actif/passif car :

- Il s'agit d'un mode de haute disponibilité nativement géré par la solution
- Ce mode correspond à notre organisation avec un fonctionnement de type nominal/secours.

Les critères retenus pour le contrôle d'intégrité des postes utilisateurs sont :

- La présence d'un antivirus activé sur le poste,
- La vérification des dernières signatures antivirales datant de moins de 5 jours
- L'appartenance du poste de l'utilisateur au parc des MEF

9 Bilan

9.1 Bilan fonctionnel

À ce stade de la rédaction du mémoire, le bilan fonctionnel est satisfaisant.

La solution a été déployée au sein des équipes techniques. Un certificat est dorénavant exigé pour accéder aux réseaux d'administration des équipements. Les informations présentes dans les certificats doivent au préalable avoir été renseignées dans les bases de l'Infranet controller pour que l'utilisateur soit autorisé à accéder au royaume « SG-ADMIN ». Ce mécanisme renforce ainsi la sécurité liée au réseau des administrateurs.

Sur le périmètre des salles de réunion, la solution fonctionne correctement. Le commutateur va détecter si le poste qui se connecte sur une prise est bien compatible avec la technologie 802.1x :

- ✓ Si c'est le cas, l'utilisateur devra envoyer, au travers de son supplicant son login et mot de passe de l'Active Directory au royaume « SG ». L'infranet controller vérifiera ces informations auprès de l'annuaire, en fonction de l'existence de son profil et des paramètres de son poste de travail, l'utilisateur se verra autorisé sur le réseau déjà paramétrer sur le port du commutateur.
- ✓ Si le poste n'est pas compatible avec la technologie 802.1x, on considère qu'il s'agit d'un visiteur qui tente d'accéder au réseau, le commutateur va automatiquement l'orienter vers le réseau visiteur d'où il pourra accéder à internet.

Pour les utilisateurs des agents du ministère, le commutateur va détecter une connexion physique sur son port. À la suite de cette connexion, une série d'échanges d'informations va avoir lieu : le supplicant installé sur le poste utilisateur va récupérer le login et mot de passe Windows de l'utilisateur et les transmettre à l'infranet controller. L'utilisateur, en fonction de l'existence de son

profil dans l'annuaire et des paramètres de son poste se verra soit affecté au réseau de quarantaine, soit autorisé sur le réseau configuré sur le port du commutateur, soit refusé.

9.2 Bilan organisationnel

D'un point de vue organisationnel, la mise en place d'une solution telle que la nôtre a un fort impact sur les processus internes propres aux équipes. Avant la mise en place de la solution, la structure de l'organisation était en silo. En effet, un utilisateur n'arrivant pas à accéder aux ressources du système d'information pour travailler, contactait auparavant le centre de services qui à son tour sollicitait l'assistance informatique de proximité.

Depuis la mise en place de la solution, l'ensemble de la chaîne support allant du centre de services, en passant par l'assistance de proximité jusqu'aux équipes support est mobilisé.

Ainsi le mode de fonctionnement transversal est dorénavant privilégié par les équipes.

Cependant, avant la mise en production de ce type de solution, il est important d'accompagner le changement par la mise en place d'ateliers de sensibilisation à l'attention de l'ensemble de la chaîne de support de l'utilisateur. Il s'agira par exemple de leur présenter l'état de l'art, de mettre en place une phase pilote pendant laquelle ils seront eux-mêmes des utilisateurs de la solution. Cela leur permettra d'adopter au quotidien les bons réflexes pour dépanner les utilisateurs.

9.3 Retour critique

Le choix organisationnel que nous avons fait est de s'équiper d'un levier supplémentaire pour la conduite d'une politique de sécurité.

L'acquisition de matériel devant se faire en fonction des contraintes d'exploitation, nous avons fait le choix de faire converger nos infrastructures.

Aujourd'hui, la direction du système d'information de l'état promeut l'acquisition de solution issue du monde libre. Cependant, ces solutions nécessitent un grand niveau de qualification des équipes en charge de leurs exploitations. Cette contrainte entraîne un fort besoin en formations des personnels utilisateurs et administrateurs.

Par ailleurs, dans les environnements d'exploitation, toutes les solutions mises en production doivent être maintenues. Pour cela, des marchés publics spécifiques liés à la maintenance sont passés.

Il en est de même pour l'acquisition de nouvelles solutions. Ainsi le risque de dépendance vis-à-vis d'un constructeur est réduit car les marchés sont renouvelés en moyenne tous les 3 ans. Avec des cycles aussi courts, l'état est contraint d'acquérir des solutions utilisant les standards du marché. Dans notre cas, les solutions basées sur le protocole 802.1x sont généralement standards. Mais lorsqu'on souhaite aller plus loin dans le contrôle du poste utilisé pour se connecter, nous sommes obligés d'utiliser des solutions propriétaires. L'adhérence créée avec le constructeur se limite au supplicant qui sera installé sur le poste de l'utilisateur.

En cas de changement de technologie, on pourra dans une première phase de migration désactiver le contrôle d'intégrité le temps que les postes utilisateur migrent vers le supplicant de la nouvelle solution.

Ainsi la solution que nous avons adoptée nous évite les coûts d'adaptation et les risques de perturbation de l'expérience utilisateur vis-à-vis du SI.

À terme, la solution de contrôle d'accès peut être améliorée pour gagner en efficacité dans la gestion du réseau en intégrant l'attribution dynamique de Vlan. L'identité de l'utilisateur déterminerait, en fonction de l'emplacement duquel il se connecte, des informations renseignées dans l'annuaire central de l'entreprise et de paramètres spécifiques à son poste, le réseau sur lequel il serait autorisé à se connecter. Dans cette optique, une étude devra être menée au préalable pour redéfinir la répartition des réseaux existants.

10 Conclusion

Avec l'expansion des usages réseaux, les exigences en matière de disponibilité des systèmes informatiques n'ont cessé de s'accroître. La croissance exponentielle de ces usages n'est pas un argument pour baisser en vigilance. Les équipes techniques doivent apporter des réponses concrètes aux besoins utilisateurs tout en leur garantissant la fiabilité des outils qui sont mis à leur disposition. Les solutions de contrôle d'accès au réseau permettent, en tant que composant du dispositif de sécurité, de répondre à ce besoin.

L'une des difficultés que j'ai pu rencontrer a été de déterminer des marqueurs pour identifier les usages des utilisateurs et ainsi pouvoir décliner la méthode d'authentification appropriée en fonction des profils.

Nous avons choisi de privilégier le mode d'authentification habituel pour les utilisateurs clients du système d'information et de rajouter un cran supplémentaire de sécurité pour les administrateurs du système d'information. Ainsi, un utilisateur utilise son Login et mot de passe pour s'authentifier sur le réseau alors qu'un administrateur du système d'information devra s'authentifier grâce à une clé cryptographique personnelle.

Pour le déploiement de la solution, nous avons dû nous y prendre de manière progressive afin de minimiser la durée et l'impact de toute interruption de service vis-à-vis des utilisateurs.

De façon plus générale, avec l'apparition de nouveaux usages tels que le BYOD, les organisations doivent renforcer les dispositifs de sécurité déjà présents sur le réseau. En s'équipant d'une solution de contrôle d'accès au réseau, les MEF anticipent les usages futurs et se dotent d'un levier non négligeable de conduite de politique et sécurité.

11 Bibliographie

11.1 Les ouvrages

Bordères, S. et N. Makarévitch. 2006. *Authentification Réseau Avec Radius : 802.1x, EAP, FreeRadius*. Eyrolles.

SGDN, Dcssi, Sdo, et BCS. 2006. « Guide 650 - La Menace Informatique. » *ANSSI*. (http://circulaire.legifrance.gouv.fr/pdf/2009/05/cir_25550.pdf).

11.2 Les documents techniques et publications

Longeon, Robert. n.d. « Un Tableau de Bord Pour Piloter La SSI. » (https://www.ljll.math.upmc.fr/interne/INFO/PSSI/doc/si8.pdf).

THONIEL, Pascal. 2017. « Méthodes D'authentification. » *Techniques de L'ingénieur Cryptographie, Authentification, Protocoles de Sécurité, VPN* base docum (Ref. article : h5535) (http://www.techniques-ingenieur.fr.proxybib.cnam.fr/base-documentaire/technologies-de-l-information-th9/cryptographie-authentification-protocoles-de-securite-vpn-42314210/methodes-d-authentification-h5535/).

CHARLOT, Cécilien. 2017. « Solutions NAC de Contrôle D'accès Au Réseau. » *Techniques de L'ingénieur Attaques et Mesures de Protection Des SI* base docum (ref. article : h5845) (http://www.techniques-ingenieur.fr.proxybib.cnam.fr/base-documentaire/technologies-de-l-information-th9/attaques-et-mesures-de-protection-des-si-42313210/solutions-nac-de-controle-d-acces-au-reseau-h5845/).

Saccavini, Luc. 2003. « 802.1X et La Sécurisation de L'accès Au Réseau Local. » (http://2003.jres.org/actes/paper.111.pdf).

Saxena, Gaurav, D. Sarkar, N. C. Samanta, and C. D. Datta. 2009. « Network Access Control : Case Study. » Calcutta : Computer & Informatics Group, VECC. (http://symposium.vecc.gov.in/sacet09/public_html/downloads/INVITED SPEAKER LECTURE/Gaurav Saxena.pdf).

2 in a Series Getting Started with Network Access Control. (http://www.opus1.com/nac/teamwhitepapers/2008-02gettingstarted.pdf).

11.3 Les sites internet

« IEEE-SA - The IEEE Standards Association. » (http://standards.ieee.org/).

« IETF Tools. » (https://tools.ietf.org/).

« Qu'est Network Policy Server (NPS) ? » (https://technet.microsoft.com/fr-fr/library/dd197558(v=ws.10).aspx).

« Juniper Networks : Juniper Networks Unified Access Control (UAC) - Contrôle D'accès Réseau, NAC, Authentification, 802.1x - Westcon Security Solutions France. » (http://fr.security.westcon.com/content/vendors/juniper/juniper-uac).

« Authentification et Mobilité (Document Destiné Aux Utilisateurs). » (http://cric.grenoble.cnrs.fr/Administrateurs/Documentations/authentification/utilisateurs.php).

Quatrième de couverture

La sécurité des systèmes d'information est un enjeu majeur pour l'État. Le protocole 802.1x est un standard permettant le contrôle de l'accès au réseau qui a été rapidement adopté sur les réseaux sans fils. En revanche, sur les réseaux filaires, la frilosité des entreprises a ralenti son expansion. Revenu au goût du jour grâce aux enjeux de sécurité de plus en plus croissants sur les réseaux internes, il peut apporter des avantages non négligeables en termes de gestion lorsqu'il est combiné avec d'autres technologies. Ce mémoire apporte une réflexion puis une solution pour renforcer le contrôle de l'accès aux réseaux informatiques filaires des Ministères Économiques et Financiers par le protocole 802.1X.

Mots-clés : 802.1X ; NAC ; RADIUS ; EAP ; Sécurité

Information technologies security is a major challenge for governments. 802.1x protocol, a standard which provides network access control, has been massively adopted on wireless networks. However, on wired networks, for different considerations many companies did not deploy this technology. Due to increasing security concerns, the protocol is back to light for wired networks and we found out that combined with other technologies, it brings significant advantages for network management. This thesis bring up a contribution to strength access control on wired network infrastructure used inside the French Economy and Finance Ministry

Key Words : 802.1X ; NAC ; RADIUS ; EAP ; Security