Ministère des Enseignements Secondaire et Supérieur
(**MESS**)

Secrétariat Général

Université Polytechnique de Bobo-Dioulasso (**U.P.B.**)

Ecole Supérieure d'Informatique (**E.S.I**)

Sadouanouan MALO

Cycle des Ingénieurs de Conception Informatique (**C.I.C.I**)

MÉMOIRE DE FIN DE CYCLE

THEME :

« Conception d'un système de sécurité : contrôle d'accès aux ressources du système d'information de la SONAPOST »

Période du 04 Novembre 2013 au 04 Mars 2014

Auteur : **KIEMDE Wênden-Tôe-Foâ Franck**

Maître de stage

M. Oscar SAVADOGO

Administrateur système à la SONAPOST

Superviseur

Dr. Sadouanouan MALO

Enseignant chercheur à l'Ecole Supérieure d'Informatique

LISTE DES FIGURES

LISTE DES TABLEAUX

SIGLES ET ABREVIATIONS

A

AAA : Authentication, Authorization and Accounting

AP: Analyse et Programmation

ACL: Control Acces list

ACS: Access Control Server

AD: Active Directory

ADFS: Active Directory Federation Services

B

BP : Boite Postale

C

CICI : Cycle des Ingénieurs de Conception Informatique

CITI : Cycle des Ingénieurs de Travaux Informatiques

CCP: Centre de Chèques Postaux

CNE : Caisse Nationale d'Epargne

D

DAC : Discretionary Access Control

DC : Direction du Courrier

DCM : Direction Commerciale et Marketing

DED : Division Etude et Développement

DG: Direction Générale

DFC: Direction Financière et Comptable

DNS : Domain Name System

DNT : Division Nouvelles technologies

DoD : Departement of Defense

DPL : Direction du Patrimoine et de la Logistique

DRC : Direction Régionale du Centre

DRN : Direction Régionale du Nord

DSI : Direction des Systèmes d'Informations

DSF : Direction des Services Financiers

DRO : Direction Régionale de l'Ouest

DRE : Direction Régionale de l'Est

DRH : Direction des Ressources Humaines

DSS : Division Support et Systèmes

ESI : Ecole Supérieure d'Informatique

FAT: file allocation table

HPFS: High Performance File System

GPO : Group Policy Object

IFS : International Financial System

IUT: Institut Universitaire de Technologie

INSSA : Institut Supérieur des Sciences de la Santé

ISEA : Institut des Sciences Exactes et Appliquées

IDR : Institut de Développement Rural

ISNV : Institut des Sciences de la Nature et de la Vie

IP: Internet Protocol

IDS: Intrusion Detection System

KDC: Key Distribution Center

LS : Liaison Spécialisée

LAN : Local Area Network

LSI: Liaisons Spécialisées avec Internet

LSS : Liaisons Spécialisées Simples

PHYSIQUE: Mandatory Access Control

MEI : Mandat Express International

NAS: Network Attached Storage

NAP: Network Access Protection

NPS: Network Policy Server

NOS: Network Operating System

NTFS: New Technology File System

NTLM: NT Lan Manager

OS : Operating System

PEAP : Protected Extensible Authentication Protocol

QoS : Quality of Service

RADIUS : Remote Authentication Dial-In User Service

RéMI : Réseaux et Maintenance Informatiques

RBAC : Role Based Access Control

RH : Ressources Humaines

SAM : Security Account Management

SG : Secrétariat Général

SID : Security Identifiers

SPN : Service Principal Name

SSO : Single Sign On

TCP: Transmission Control Protocol

TDO: Trusted Domain Object

UPB : Université Polytechnique de Bobo-Dioulasso

UPN : User Principal Name

VLAN : Virtual Local Area Network

WAN : Wide Area Network

DEDICACE

- A mes parents qui n'ont jamais cessé de me soutenir tout au long de mes études ;
- A mes très chers frères, sœurs et amis pour leur soutien et leur encouragement.

Qu'ils trouvent ici le témoignage de ma très grande affection

« Qui nous séparera de l'amour de Christ ? Sera-ce la tribulation, ou l'angoisse, ou la persécution, ou la faim, ou la nudité, ou le péril, ou l'épée ?... Car j'ai l'assurance que ni la mort ni la vie, ni les anges ni les dominations, ni les choses présentes ni les choses à venir, ni les puissances, ni la hauteur, ni la profondeur, ni aucune autre créature ne pourra nous séparer de l'amour de Dieu manifesté en Jésus-Christ notre Seigneur. »

Romains 8 v 35-39

REMERCIEMENTS

Sans le concours de certaines personnes, notre travail de recherche ne saurait être concluant. C'est pourquoi, nous manifestons de travers ces lignes, notre profonde gratitude et notre reconnaissance à tous ceux qui ont contribué à la réalisation de ce travail. Nous remercions particulièrement à :

- l'Ecole Supérieure d'Informatique (ESI) pour toute la formation que j'ai reçue.
- Monsieur le Directeur BAHORO Sïaka de la Direction du Système Informatique (DSI) pour m'avoir permis de réaliser mon stage dans sa direction.
- Monsieur Oscar SAVADOGO, mon maître de stage qui a toujours été à l'écoute et qui a su m'apporter de judicieux conseils.
- Monsieur Saïdou OUEDRAOGO, pour m'avoir soutenu dans la réalisation de mon stage et la rédaction du rapport.
- Monsieur Yacouba KABORE et Monsieur Kévin MILLOGO pour m'avoir éclairé l'esprit sur certaines zones d'ombre concernant le système d'information.
- la grand-mère Marie OUEDRAOGO, enfants et petits-enfants pour leur soutien inestimable et continuel à mon égard tout au long de mes études.

Enfin, je remercie du fond du cœur le Docteur MALO Sadouanouan, mon superviseur pour m'avoir guidé et donné des directives précieuses tout au long de mon stage.

Toute ma révérence à Dieu pour tous ses bienfaits

AVANT-PROPOS

Ce mémoire est réalisé dans le cadre de l'examen final de l'Ecole Supérieure d'Informatique (ESI) de l'Université Polytechnique de Bobo-Dioulasso (UPB), en vue de l'obtention du titre d'ingénieur de conception en informatique. Il correspond au travail effectué à la Division Support et Systèmes (DSS) de la Direction des Systèmes d'Information (DSI) de la Société Nationale des Postes (SONAPOST) du Burkina Faso du 04 Novembre 2013 au 04 Mars 2014, présenté et soutenu le 09 Décembre 2014, sous la supervision du Docteur MALO Sadouanouan enseignant chercheur à l'Ecole Supérieure d'Informatique (ESI).

Avec l'ère du numérique, toute une variété de nouveaux défis techniques, scientifiques et sociaux sont apparus. L'un d'entre eux est la sécurité des systèmes d'information. Alors que nous incluons tout dans les problèmes de sécurité, les logiciels malveillants ou le courrier indésirable qui polluent nos environnements de travail, les grandes entreprises redoutent la mise hors d'usage de leurs systèmes de production et la fuite d'informations confidentielles. Les enjeux de la sécurité sont devenus tellement important, image de marque, pertes financières directes ou indirectes massives, etc., que des moyens considérables sont investis pour garantir la sécurité des systèmes. Cette sensibilisation croissante aux notions de sécurisation des systèmes d'information des entreprises, a conduit les administrateurs système à devoir répondre à de nouveaux types d'exigences : le contrôle d'accès aux ressources du système d'information.

La notion de contrôle d'accès est bien antérieure à l'informatique : de tout temps des gardes, des chaînes et des herses ont été dressées pour protéger des accès illégitimes. Les recherches dans le domaine du contrôle d'accès furent initiées par le « Departement of Defense » américain (DoD) dans les années 70. Des modèles théoriques furent élaborés et très largement implantés, pour faire face aux besoins de sécurité militaire de l'époque. Avec la démocratisation de l'informatique et son usage incontournable dans presque toutes les organisations, tous les acteurs de l'informatique prêtent désormais attention à la sécurité de leurs systèmes d'information.

La Société Nationale des Postes du Burkina Faso (SONAPOST) ne reste pas indifférent à cela. Elle cherche à renforcer la sécurité des accès à son système d'information. C'est dans cette vision que nous avons effectué des travaux d'analyse et de conception, pour l'implémentation d'un système de contrôle d'accès aux ressources du système d'information de la SONAPOST. Cette étude a porté sur une analyse du système d'information de la SONAPOST (traitant de la gestion des ressources), suivie de celle du contrôle d'accès (en ces principes de fonctionnement) et enfin celle des concepts fonctionnels et techniques du système de contrôle d'accès (que nous intégrerons dans le système d'information de la SONAPOST).

Introduction

Dans ce chapitre, il s'agit de mettre notre travail dans son contexte général. La première section comprend alors la présentation des structures d'accueil et la deuxième, une brève description de la méthodologie du travail adoptée suivie de la gestion du projet nécessaire pour le déroulement de notre travail.

Le système d'information de la SONAPOST est un agrégat de domaines Windows indépendant sur un même réseau informatique. Cette disparité du système d'information engendre des déficiences d'administration et de sécurité. En effet, il est devenu un point critique de la société, qui est régulièrement amenée à perdre des heures considérables de travail dès lors que celui-ci n'est plus accessible. En ajoutant à cela, la fréquence des pertes de données dues à la mauvaise manipulation des utilisateurs et l'augmentation de l'activité virale. Le besoin d'unification des domaines en un seul, est devenu nécessaire pour garantir plus de fiabilité et de sécurité au sein du système d'information.

L'aspect majeur de cette entreprise est d'assurer la disponibilité, l'intégrité et la confidentialité des ressources du système d'information sur l'ensemble du réseau informatique. Au-delà de son aspect fonctionnel, l'infrastructure réseau est d'un accès particulièrement critique pour la sécurité des entités du système d'information. Les plus sensibles sont les serveurs d'application et d'administration, qui stockent les informations les plus confidentielles de la société. Qu'il soit filaire ou non, le réseau est accessible dès lors qu'on est dans les locaux de la société. N'importe qui ne devant pas avoir la possibilité de se connecter au système information, il faut mettre en place un mécanisme de contrôle logique pour restreindre l'accès au réseau. Pour autant, ce mécanisme ne doit pas être lourd à administrer, ce qui impliquerait rapidement un laxisme et une confusion dans les règles établies. Définir strictement les autorisations en fonction des points d'accès physiques pour ensuite établir une carte des autorisations de l'ensemble des bâtiments, n'est pas non plus la bonne solution, puisqu'il sera difficile de garantir les contrôles d'accès à ces prises.

L'utilisation du réseau dépendra également de l'emplacement géographique de l'utilisateur, à l'encontre de toute logique vis-à-vis de la tendance actuelle au nomadisme constaté dans les entreprises.

Pour répondre à toutes ces exigences critiques, et garantir l'intégrité du réseau et la confidentialité de ses données (tout en sauvegardant la liberté de mouvement de ses employés), la Direction des systèmes d'informations (DSI) est contrainte d'exploiter les nouvelles technologies les plus adéquates. De nouveaux outils d'administration doivent donc être développés, pour pouvoir être proposés aux utilisateurs. Au-delà du déploiement des politiques de sécurisation, il est souhaitable d'offrir une souplesse d'administration exemplaire du système, en permettant aussi bien aux employés de modifier aisément les permissions sur certaines ressources. C'est ainsi que le thème : « ***Conception d'un système de sécurité : contrôle d'accès aux ressources du système d'information, cas de la SONAPOST »,*** nous a été soumis dans le cadre de notre stage au sein de la DSI de la SONAPOST. Avec pour objectif la mise en place d'un système de sécurité permettant de protéger les ressources du système d'information d'un accès ou d'un usage non autorisé depuis l'intérieur, par un inconnu ou un utilisateur inapproprié, avec quelque outil que ce soit. Ceci passe par le contrôle d'accès au réseau de la société, à ses applications et aux données. Avant d'aborder la suite de nos travaux, nous présentons l'Ecole Supérieure d'Informatique (ESI) et la Société Nationale des Postes (SONAPOST).

Présentation de l'Université Polytechnique Bobo-Dioulasso

L'Université Polytechnique Bobo-Dioulasso (**UPB**) est un établissement public de l'Etat à caractère scientifique, culturel et technique chargé de l'enseignement supérieur et de la recherche scientifique. Elle jouit de la personnalité morale et de l'autonomie scientifique, administrative et financière. L'UPB comprend des écoles et des instituts. Elle a pour mission fondamentale la recherche de la connaissance et sa transmission en formant des hommes et des femmes pour les besoins de la nation. Pour ce faire, elle poursuit les objectifs suivants :

- former des cadres dans tous les domaines en général et dans les filières professionnalisantes en particulier ;
- conduire des activités de recherche scientifique et en vulgariser les résultats;

- élever le niveau technique, scientifique et culturel des travailleurs ;
- contribuer au développement économique, social et culturel du pays notamment en participant de façon efficiente a une ouverture sur le marché de l'emploi et aux secteurs de production ;
- délivrer des titres et des diplômes ;
- valoriser les compétences dans tous les secteurs d'activités du pays;
- coopérer en matière de formation recherche et promouvoir les échanges interuniversitaires.

L'UPB comprend une école et cinq (5) instituts placés chacun sous la responsabilité d'un directeur. On a : L'Ecole Supérieure d'Informatique (ESI), l'Institut Universitaire de Technologie (IUT), l'Institut du Développement Rural (IDR), l'Institut des Sciences de la Nature et de la Vie (ISNV), l'Institut des Sciences Exactes et Appliquées (ISEA) et l'Institut Supérieur des Sciences de la Santé (INSSA).

L'Ecole Supérieure d'Informatique (ESI) a été créée en 1991 suite au besoin exprimé par le Premier Plan Directeur Informatique (PPDI) (1991-1995) dont un des objectifs est « édification de compétences nationales par la formation de spécialistes (analystes et ingénieurs) concepteurs de système d'information ».

Initialement logée au sein de l'Université de Ouagadougou, elle est installée de nos jours à l'Université Polytechnique de Bobo-Dioulasso et offre trois types de formations :

- le Cycle des Ingénieurs de Travaux Informatiques (CITI), qui comporte deux filières:
  - la filière Analyse et Programmation (AP)
  - la filière Réseaux et Maintenance Informatiques (RéMI).
- le Cycle des Ingénieurs de Conception Informatique (CICI), qui est notre cycle de formation.

La société nationale des postes (SONAPOST) est un établissement public à caractère industriel et commercial (EPIC). Il est chargé de l'exploitation du service public des postes ainsi que de la promotion et de la mobilisation de l'épargne. Elle est engagée dans un projet de croissance dynamique et rentable par l'élaboration d'un plan stratégique de développement. Fidèle à l'idée de progrès social qui présida

à sa création, la Poste aujourd'hui conjugue bien croissance et performance, innovation technologique et satisfaction de la clientèle. La SONAPOST, premier réseau de contact au Burkina Faso emploie actuellement plus de 942 personnes avec plus de 400 guichets et 97 bureaux de postes sur le territoire national.

La Société Nationale des Postes (SONAPOST) a pour objectif, pour son compte ou pour le compte de tiers, au BURKINA FASO:

- d'assurer dans les relations intérieures ou internationales le service public du courrier dans toutes ses formes ;
- d'assurer directement ou indirectement toute autre activité liée à son objet ;
- d'assurer la mobilisation et la promotion de l'épargne, le règlement des valeurs effets et virements postaux ;
- d'offrir les prestations relatives aux moyens de paiement et de transfert de fonds aux produits de l'épargne et des chèques postaux ;
- d'assurer toute activité financière compatible avec la gestion des services financiers postaux ;
- d'appliquer la législation et la réglementation propres aux Postes et les conventions, règlements et arrangements de l'Union Postale Universelle et des unions restreintes dont le BURKINA FASO est membre ;
- préparer et d'exécuter les plans d'équipement des Postes.

La SONAPOST, pour répondre à son objectif et s'inscrire dans une politique de développement économique, œuvre dans divers domaines : le domaine du courrier, le domaine des finances et le domaine des nouvelles technologies

3.2.1 Le domaine du courrier

Le domaine du courrier est reparti selon les activités postales suivantes :

- La boîte postale : qui est l'adresse officielle et légale d'une personne physique ou morale et à laquelle son courrier lui est adressé ;

- Le colis postal : qui constitue le circuit d'approvisionnement, d'achat et de vente par correspondance de la poste ;
- La machine à affranchir : qui est un mode d'acquittement de la taxe de port très pratique mis à la disposition des particuliers et des personnes morales ayant des quantités importantes de courriers à expédier ;
- Le Post 'Eclair : qui est un service de collecte, de traitement et de distribution rapide à délais garantis des lettres, documents, paquets, cadeaux ... à Ouagadougou et partout au Burkina ;
- Le publipostage : qui consiste à mettre en relation une entreprise et des clients au moyen de messages publicitaires sous pli ou à découvert dont la distribution se fait en boîte postale.

3.2.2 Le domaine des finances

Le domaine des finances est reparti selon les activités financières suivantes :

- Le mandat Teliman : qui est un système de transfert électronique d'argent reliant tous les bureaux de la Poste à travers tout le Burkina Faso ;
- L'épargne : par le moyen du compte local et l'épargne retraite Poste ;
- Les chèques postaux : à travers le Centre des Chèques Postaux, en abrégé CCP, est chargé de la gestion des comptes courants ;
- Western Union : utilisé dans tous les bureaux de la Poste pour envoyer et recevoir de l'argent.

3.2.3 Le domaine des nouvelles technologies

Le domaine des nouvelles technologies est chargé des activités suivantes :

- Les cyberpostes: permettant d'offrir la connexion à Internet dans plusieurs villes du pays dans ses cybercafés dénommés Cyberpostes ;
- Le Cyberkiosque : qui est un projet pilote, offrant un accès à Internet haut débit par liaison satellitaire. L'équipement est composé d'un ordinateur à écran tactile, d'un clavier, d'une souris et d'une webcam incorporée. Il permet de recevoir ou d'émettre un appel audio et vidéo.

3.3 Organisation et fonctionnement

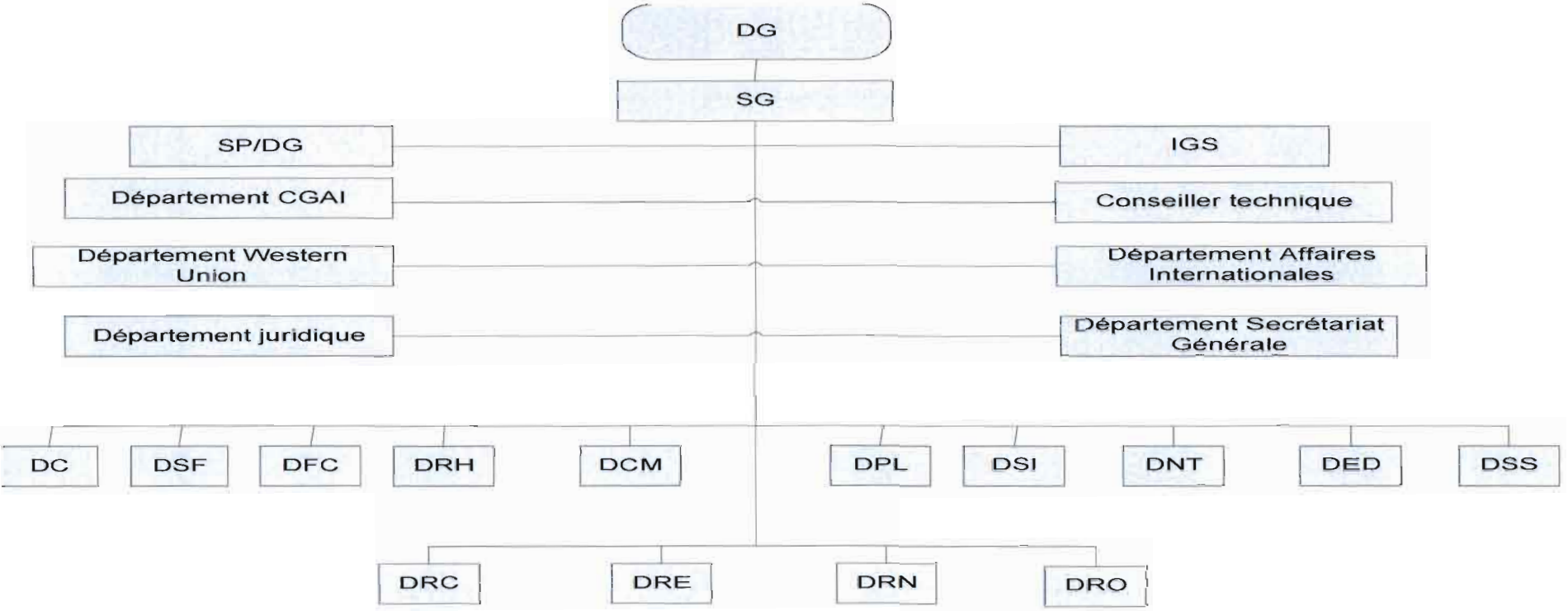


Figure 1 : l'organigramme de la SONAPOST

3.3.1 L'administration centrale

L'administration centrale se compose de :

- **La Direction Générale (DG)**

Le Directeur Général est chargé de la direction technique, administrative, commerciale et financière de la société.

- **Le Secrétariat Général (SG)**

Le Secrétaire Général assiste le Directeur Général dans toutes les questions techniques et d'administration générale. Il assure l'intérim du Directeur Général.

- **Les directions et services rattachés**

Ils ont pour attributions l'organisation, l'animation du réseau de développement et de la gestion des activités et ont en charge les missions d'inspection technique et d'assistance.

- **Les directions techniques**

Elles sont les suivantes:

- **La Direction du Courrier (DC),**
- **La Direction des Services Financiers (DSF),**
- **La Direction Financière et Comptable (DFC),**
- **La Direction des Ressources Humaines (DRH),**
- **La Direction du Patrimoine et de la Logistique (DPL),**
- **La Direction Commerciale et Marketing (DCM),**
- **La Direction des Systèmes d'Information (DSI).**

Nous avons effectué notre stage au sein de la Direction des Systèmes d'Information (DSI). Elle est le centre des ressources informatiques et est composée de trois (03) divisions dont les attributions sont indiquées dans le tableau 1 suivant.

Tableau 1: les divisions de la DSI

Division	Attributions
Division Support et Systèmes (DSS)	Administration des systèmes informatiques (systèmes, base de données...) ; -mise en place des procédures de sécurité des données, des systèmes et des lieux ; - la mise en place d'une politique de sauvegarde des données; - l'extension du réseau informatique ; - la formation et l'assistance des utilisateurs; - la gestion du matériel, etc.
Division Nouvelles Technologies *(DNT)*	-Mise en place de l'infrastructure de base pour l'accès Internet; - Mise en place de l'intranet/extranet de la société; - Amélioration de la visibilité de la société relativement aux services offerts; - le développement des nouveaux produits liés à l'Internet; - l'administration du réseau.
Division Etude et Développement *(DED)*	-Le déploiement des logiciels; - La formation des utilisateurs; - la maintenance des applications; - la conception et mise à jour du site web de la société.

3.3.2 Les directions régionales

Les directions régionales sont chargées de l'organisation, de l'animation et de la supervision des structures postales qui leur sont rattachées, ainsi que de la gestion du patrimoine de la société dans leur ressort territorial. De façon générale, elles sont chargées de la mise en œuvre de la politique de la société définie par la direction générale. Les directions régionales sont :

- la Direction Régionale du Centre (DRC) dont le siège est à Ouagadougou ;
- la Direction Régionale de l'Ouest (DRO) qui a pour siège Bobo-Dioulasso ;
- la Direction Régionale de l'Est (DRE) dont Fada N'Gourma est le siège ;
- la Direction Régionale du Nord (DRN) qui a pour siège Ouahigouya.

3.3.3 Les centres spécialisés

Les centres spécialisés sont des centres dont la vocation est de traiter des opérations spécifiques de contrôle ou d'exploitation ou d'assurer une mission de formation. Ils sont rattachés à une direction technique ou à une direction régionale (mais la plupart reste rattachés à des directions régionales).

3.3.4 Les bureaux de poste

Les bureaux de poste ont pour vocation le traitement des opérations spécifiques d'exploitation. Ils sont aux nombres de 97 avec une moyenne de 4 guichets par bureau.

4.1.1 Description

L'évolution des technologies de l'information et de la télécommunication a apporté une véritable révolution des systèmes d'information dans les entreprises. De l'acquisition des informations, de leur traitement à leur stockage, il est défini des processus propres à chaque entreprise en vue d'assurer la disponibilité, l'intégrité, la confidentialité et l'authenticité de l'information. L'information étant la véritable ressource et l'essence même d'une entreprise, celle-ci doit être protégée, de même que toute source ou objet pouvant participer à son élaboration de façon directe ou indirecte, de tout accès non autorisé ou de tout usage non approprié. Les enjeux qui y sont associés sont considérables, au point qu'une légère négligence peut paralyser l'ensemble des activités de l'organisation.

Pour le cas de la SONAPOST qui fait l'objet de notre étude, avec un capital de plus 38 milliards de F CFA, une Caisse Nationale d'Epargne (CNE) gérant plus de 458.612 comptes pour un avoir global de plus de 84 909 564 652 FCFA, un Centre des Chèques Postaux (CCP) de plus de 4 265 comptes pour un avoir global de 68 892 698 521 FCFA, un parc de plus de 31 757 boîtes postales, un réseau de 119 coursiers cyclistes et un parc de machines à affranchir est à protéger. Tout cela montre qu'il est nécessaire et impérieux de se doter d'une sécurité robuste conséquente. C'est fort de ce constat, et conscients que

80% des menaces de la sécurité d'un système d'information viennent de l'intérieur et qu'aucun système ne peut être sécurisé à 100%, que nous avons été investis du thème intitulé: *«Conception d'un système de sécurité : contrôle d'accès aux ressources du système d'information, cas de la SONAPOST».* Entendons ici par ressource, tout composant (physique ou logique) participant à l'élaboration, au traitement, à la transmission et au stockage des données dans le système d'information.

Par ce thème, nous ambitionnons de contribuer à la consolidation des dispositifs mis en œuvre pour restreindre les menaces et les dangers pesant sur les ressources du système d'information de la SONAPOST. En effet, réduire les risques encourus par l'organisme du fait de son système d'information est le but premier recherché par le contrôle d'accès qui va constituer essentiellement l'objectif de notre étude qui est de garantir la sécurité et l'intégrité des ressources du système d'information de la SONAPOST.

4.1.2 Analyse de risque

Les risques de la non mise en place du système sont multiples. On peut citer entre autres :

- les risques d'infection par virus depuis un ordinateur externe ;
- les risques de piratage du système à travers un ordinateur interne ;
- les risques de vol d'informations sensibles ;
- les risques de mauvais fonctionnements ou de pannes du réseau de la société

4.2.1 Description

La finalité de ce projet est la mise en place d'un système de sécurité permettant de protéger les ressources du système d'information, d'un accès ou d'un usage non autorisé par un inconnu ou un utilisateur inapproprié, avec quelque outil que ce soit. Cette protection est basée sur le contrôle des accès aux ressources du système information par les machines et les utilisateurs, ceci passe par le contrôle d'accès au réseau de la société, à ses applications et aux données. Ce qui implique que chacun des utilisateurs du système

d'information doit être individuellement suivi par rapport au respect de la sécurité du système et du réseau de la société, des applications et des données. Il s'agira de protéger :

- l'infrastructure interne d'une intrusion depuis l'intérieur par la connexion d'un poste incorinu sur le réseau de la société.

Cette protection doit être réalisée en séparant les différents périphériques dans des réseaux différents de manière à ce que les ordinateurs professionnels, présents dans l'annuaire Active Directory de la société, soient dans un réseau qui leur permet l'accès à toutes les ressources de la société et que les ordinateurs « inconnus » soient dans un réseau leur permettant uniquement l'accès à internet.

De plus, un équipement réseau « non-validé » tel qu'un Switch par exemple, ne doit pas pouvoir mettre en péril l'intégrité et le bon fonctionnement du réseau global de l'entreprise.

- les ressources système d'un usage inapproprié par un utilisateur non autorisé au sein du système informatique de la société.

Cette protection doit être réalisée en permettant uniquement aux utilisateurs, présents dans l'annuaire Active Directory de la société et conformément à une politique de contrôle d'accès, d'accéder au système d'information (ou à une partie du système) et de pouvoir utiliser les ressources disponibles dans cette partie (applications, imprimantes, fichiers, etc.).

En plus, le redéploiement humain (la mobilité des utilisateurs) comme les mutations et les promotions en exemple, ne doit pas nuire à l'intégrité, à la confidentialité et à la disponibilité des ressources systèmes et de façon générale à la politique de contrôle d'accès.

4.2.2 Exigences globales du futur système

Pour y arriver, nous définissons les exigences globales suivantes :

- Les postes ordinateurs de la société doivent avoir accès à l'infrastructure interne du système d'information de la société ;

- Les postes ordinateurs externes doivent avoir accès uniquement à internet ;
- Les imprimantes de la société doivent être autorisées par défaut ;
- Les téléphones IP de la société doivent être autorisés par défaut ;
- L'accès d'un réseau à l'autre doit être restreint ;
- Les mêmes règles doivent s'appliquer en cascadant un PC ou un Switch derrière un téléphone IP ;
- Le personnel de la société doit pouvoir se connecter au système d'information;
- Le personnel de la société doit être affilié à une politique de contrôle d'accès (authentifié, autorisé et journalisé) sur leurs accès au système d'information et à ses ressources.

A cette fin, il nous est nécessaire d'établir une démarche à suivre pour mieux explorer tous les aspects sécuritaires possibles en contrôlant des accès sur le système d'information.

De la description des exigences globales, nous faisons une analyse technique du futur système comme suit :

- Les ordinateurs professionnels dans un groupe de sécurité « comptes ordinateurs » ;
- Les équipements « autorisés » (ordinateurs professionnels et imprimantes de la société) dans un même VLAN ;
- Les téléphones IP « autorisés » dans un VLAN différent (VLAN voix) ;
- Les équipements « externes » (ordinateurs externes) doivent être dans un VLAN « Guest » leur donnant accès uniquement à internet ;

- Les équipements « nomades » (Switch non validés ou tout autre équipement réseau) seront traités de la même manière que les équipements « externes » ;
- Les utilisateurs dans le groupe « comptes utilisateurs », avec des comptes utilisateur de type standard;
- Les utilisateurs accédant « autorisés » à une même ressource, dans un sous-groupe spécifique du groupe utilisateur ;
- Les fichiers partagés dans un serveur de fichier ;
- Les profils utilisateurs dans un NAS (Network Attached Storage).

La réalisation de ces objectifs en conformité avec les principes de contrôle d'accès, est assurée par des mécanismes de contrôle d'accès logique. Les mécanismes de contrôle d'accès physique et administrative ne seront pas traités car n'étant pas partie des attributions du projet. Le contrôle d'accès à une ressource du système d'information est assuré suivant deux modes :

- le Mode à priori : qui consiste à l'audit et la configuration des droits d'accès attribués aux utilisateurs (on parle de "gestion des identités et des habilitations") ;
- le Mode à posteriori : se rapportant au contrôle des droits d'accès attribués aux utilisateurs et aux équipements au moment de l'accès au système (on parle de "contrôle d'accès au réseau et service").

Suivant le mode de contrôle d'accès, plusieurs concepts fondamentaux interviennent dans la réalisation du contrôle d'accès aux ressources du système d'information.

5.2.1 Gestion des identités et des habilitations

La gestion des identités et des habilitations fournit une vue sur l'ensemble des droits d'accès dont dispose un utilisateur (ou groupe utilisateurs) ou un équipement réseau dans le système d'information. Conformément à la modélisation du modèle de la politique de contrôle d'accès basée sur les rôles (RBAC), adopté lors de la mise en place du projet au sein de l'annuaire Active Directory. L'objectif étant de doter :

- les utilisateurs, que des droits d'accès nécessaires (principe du moindre privilège) pour l'exécution de leurs fonctions au sein de la SONAPOST. Un utilisateur dans le système d'information n'aura pas accès à toutes les ressources. Ainsi un utilisateur extérieur n'aura pas accès aux ressources ;

- les équipements réseau, que des « droits de connexion et d'opération » nécessaires pour assurer la disponibilité, l'intégrité et confidentialité des ressources du système. Un équipement réseau ne pourra pas communiquer avec tous les équipements du réseau.

5.2.2 Contrôle d'accès au réseau et service

Le contrôle d'accès est réalisé par l'implémentation des trois propriétés importantes de la fonction de sécurité des systèmes informations « les 3A » (**A**uthentication, **A**uthorization, **A**ccounting), suivant une stratégie de sécurité informatique. Dans notre cas, la stratégie de la défense en profondeur fut adoptée. Le système de contrôle d'accès est ainsi subdivisé en trois périmètres de contrôle, que sont : le contrôle d'accès réseau, le contrôle d'accès au système d'exploitation et le contrôle d'accès aux données.

- Le contrôle d'accès réseau, est un contrôle des équipements réseau accédant au système grâce au réseau informatique. Il vérifie l'identité et l'autorisation des différents équipements réseau et la place dans leur VLAN respectif. Il est chargé en aval d'alerter les tentatives d'intrusions et de dissuader les pirates et les utilisateurs inconnus. Ce contrôle s'exécute sans l'aval de l'utilisateur, lors de la connexion sur le réseau.

- Le contrôle d'accès au système d'exploitation, est un contrôle de l'ouverture de la session d'un utilisateur. Ce contrôle permet ou non l'accès à l'ensemble des services supportés en amont aux serveurs suivant le profil de l'utilisateur. Il veille à authentifier et à autoriser les utilisateurs accédant au système d'information lors de l'ouverture d'une session. Pour y arriver, nous avons adopté l'usage de mécanisme d'authentification et d'autorisation qu'offre le contrôleur de domaine avec l'annuaire Active Directory. Ce contrôle est chargé de gérer l'ouverture d'une session de l'utilisateur suivant son profil dans le système, une fois le contrôle d'autorisation satisfait. En aval, il est chargé d'alerter les intrusions et à l'utilisateur ses besoins de conformité à la politique de sécurité et de dissuader les pirates et les utilisateurs inconnus.

- Le contrôle d'accès aux données (dossier, fichier, application, etc.), est un contrôle des droits des utilisateurs sur les ressources du système d'information. Il délimite les droits qu'a un utilisateur lors des manipulations des ressources. Le contrôle s'effectuera sur les droits (permissions) que possède un utilisateur sur une ressource donnée.

Les connexions doivent être traçables dans un log avec indication de nom de l'équipement client, adresse physique, adresse IP, date, heure, accès autorisé ou refusé et le Switch sur lequel a eu lieu l'accès.

Les acteurs identifiés pour ce projet sont le groupe de pilotage, le groupe du projet et le groupe des utilisateurs.

- Le groupe de pilotage : ce groupe a pour rôle d'arbitrer et de contrôler les décisions à prendre. Il valide les grands choix techniques et fonctionnels, fixe les orientations générales et les délais d'exécution, définit les moyens à mettre en place pour la réalisation du projet et approuve le plan d'action établi par le groupe de projet. Il est constitué de l'ensemble du personnel de la Direction du Système d'Information(DSI) de la Poste.
- Le groupe de projet : ce groupe est chargé de l'exécution du projet c'est-à-dire, de l'étude préliminaire à la mise en place de la plate-forme. Il établit également des rapports sur l'activité et l'avancement du projet auprès du comité de pilotage. Ce groupe de projet est composé de :
    - Monsieur SAVADOGO Oscar, chef de la division support et systèmes à la Direction du Système d'Information(DSI) de la Poste.
    - KIEMDE Wênden-tôe-fôa Franck, Etudiant en deuxième année du Cycle des Ingénieurs de conception en Informatique à l'Université Polytechnique de Bobo-Dioulasso,
- Le groupe des utilisateurs : ce groupe a pour objectif de valider les éléments de l'étude relevant de son domaine de compétence. Il devra faire connaitre ses attentes face au projet à réaliser. Il est composé de l'ensemble des administrateurs systèmes de la Direction des Systèmes d'Information (DSI) et des agents de la SONAPOST.

6.2 Le planning prévisionnel

Nous effectuerons d'abord une analyse critique de l'ensemble du système de contrôle d'accès actuel et celle des besoins d'accès des utilisateurs. Ensuite, l'élaboration du système de contrôle des accès, sur laquelle nous définirons des stratégies générales de contrôle d'accès, et des technologies de mises en œuvre. Enfin nous établirons des politiques de sécurité et la phase de transition du système de contrôle des accès aux ressources du système d'information. Le tableau suivant ci-dessous décrit la planification prévisionnelle de la réalisation du projet.

Tableau 2 : Planification du projet

Période / Etapes	Novembre			Décembre			Janvier			Février			Livrables
	01	10	20	30	10	20	31	10	20	31	10	20	28	
I														Etude du cahier des charges
II														Etude de l'existant
III														Plateforme
IV														Rapport sur projet

Conclusion

L'étude préliminaire, nous a permis de découvrir l'environnement et le contexte du projet et ses attentes. A la suite de cette étude, nous avons décelé les exigences globales du système futur, que nous mettons dans le contexte de notre projet d'étude.

Il devient donc important pour nous, pour pallier ces exigences d'avoir une vue globale sur l'ensemble du système d'information de la SONAPOST.

Introduction

L'étude de l'existant est une partie essentielle de notre travail. En effet, nos analyses et remarques éventuelle sur le système de contrôle d'accès, ne peuvent qu'être basées sur cette partie «existant ». Il nous faut donc connaître parfaitement le système d'information, car le niveau de sécurité d'un système se réduit au niveau de sécurité de son maillon le plus faible.

Le réseau de la SONAPOST est un réseau Ethernet bâti sur le model architectural TCP/IP. Le réseau s'étend sur l'ensemble des régions du pays. il offre ainsi un support fiable à l'exploitation des services du système d'information, et Il regroupe en son sein plusieurs réseaux LAN interconnectés par divers moyens d'interconnexion.

Le réseau informatique de la SONAPOST est réparti sur tout le territoire national. Il est composé de plusieurs réseaux Ethernet, et compte précisément vingt(20) sites dont neuf (9) à Ouagadougou et onze (11) dans les autres provinces.

Tableau 3 : les sites de la SONAPOST

Sites voisins du siège (8)	Sites Distants (11)
Siège-Aéroport, Siège –Zogona, Siège - Building-Lamizana, Siège -Dassasgho, Siège -Nimnin, Siège -Goughin, Siège - Patte-d'oie, Siège -1200 logements.	Bobo-RS, Bobo-Hamdalaye, Bobo – Nieneta, Banfora, Fada-N'gourma, Garango, Koudougou, Koupela, Ouahigouya, Tenkodogo, Yako.

La SONAPOST utilise des liaisons spécialisées pour interconnecter l'ensemble de ses sites au siège. Au total nous avons vingt et une (21) liaisons spécialisées (LS) dont douze (12) avec connexion à Internet (LSI) et neuf (9) sans connexion internet, encore

appelées liaisons spécialisées simples (LSS). Un réseau VPN (Virtual Private Network) est implémenté pour permettre aux sites utilisant des LSI de se connecter au site siège de façon sécurisée. Pour protéger l'ouverture du réseau sur Internet, des firewalls sont mis en place. En effet, pour les sites utilisant la LSI, des firewalls sont placés à l'entrée de chaque réseau local tandis que ceux utilisant la LSS passent par le firewall principal du siège.

Des descriptions précédentes, nous pouvons à présent faire une synthèse schématique du réseau de la SONAPOST réparti dans près d'une dizaine de provinces.

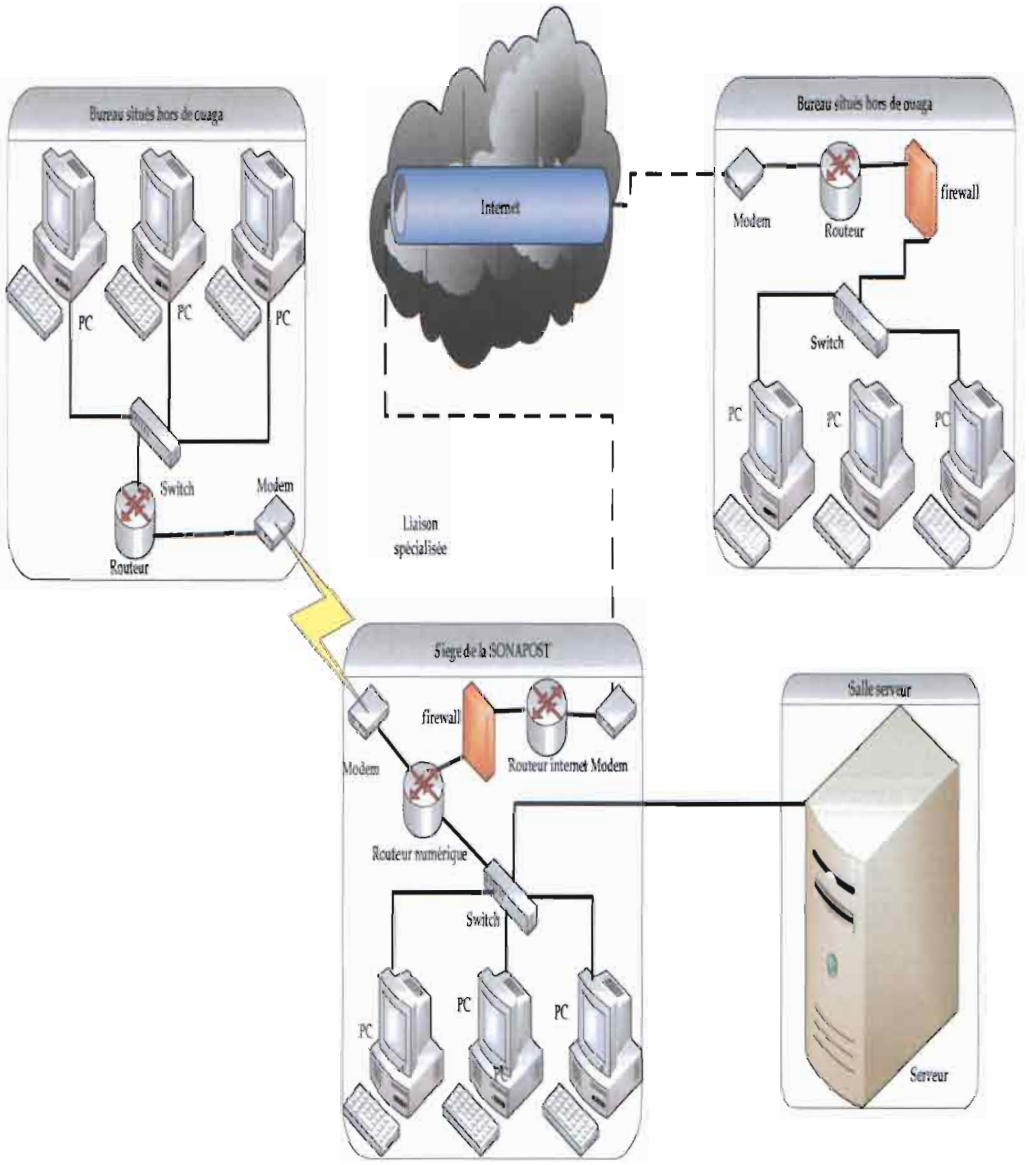


Figure 2 : Schéma récapitulatif du réseau de la SONAPOST

❖ **Les équipements d'interconnexion utilisés**

Dans l'ensemble, nous avons pour les différents sites, un modem, un routeur pour l'interconnexion au siège, des concentrateurs ou des commutateurs pour la gestion interne des ordinateurs du réseau local.

❖ **L'adressage du réseau**

La répartition du réseau de la SONAPOST est d'abord faite par son agencement géographique. Chaque site géographique représente un réseau. Les classes d'adresse A, B et C sont toutes utilisées dans le réseau.

Une segmentation logique vient faciliter l'administration ce vaste ensemble interconnecté. Cette division logique est aussi un plus pour la sécurité car elle permet un meilleur contrôle du trafic réseau.

[illegible]

L'infrastructure du système informatique de la SONAPOST est bâtie sur la technologie Windows. Elle est composée de quatre Domain Windows, tous indépendants sans approbation de forêt (laposte.bf ; sonapost.com ; sona-ips.lan et laposte.lan) et d'un ensemble de systèmes d'application, de sauvegarde, de base de données et de fichiers. L'ensemble de ces entités sont installées sur des serveurs qui leurs sont dédiés et qui sont hébergés à la direction générale, au sein d'un VLAN spécifique, accessible sur tous les sites géographiques de la SONAPOST.

Pour accéder aux ressources et aux services fournis par les différentes applications et les serveurs de fichiers, l'utilisateur passe sous le contrôle des contrôleurs de domaine qui les abritent. Chaque domaine offre aux utilisateurs (authentifiés) un accès direct (autorisation) à des ressources telles que les fichiers partagés et les applications. L'utilisateur pour s'authentifier, se logue sur sa machine (login + mot de passe) en local. Il utilise les navigateurs Web et les clients lourds pour l'exploitation des applications. Cependant, l'exploitation des applications reste conditionnée par un login et un mot de passe de l'utilisateur, stockés dans la base de données de l'application, servant à l'authentification de l'utilisateur. Les machines sont connectées au réseau, sur des VLAN de niveau trois(3) permettant d'accéder aux applications, aux serveurs de fichiers.

2.1.1 Les serveurs applicatifs

Nous appelons serveurs applicatifs ceux qui sont directement liés à la gestion automatisée des activités de la SONAPOST. Ce sont :

- Le serveur IFS (International Financial System) hébergeant l'application IFS utilisée dans les transactions électroniques.
- Le serveur CCP (Centre de Chèques Postaux) hébergeant l'application de comptabilité CCP.
- Le serveur BP (Boite Postale) : Gère les payements et les résiliations des clients de Boîte Postale;
- Le serveur BD Orale: Hébergement de la base de données du service Boîte Postale
- Le serveur RAS WU : Gère les transferts Western Union;
- Le serveur de Développement Oracle (Serveur test) : Permet d'interpréter des scripts et de les traduire en requêtes SQL afin d'interroger le serveur de base de données Oracle.
- Le logiciel CNE (Caisse Nationale d'Epargne) : Gère les comptes CNE.
- Le logiciel Teliman de transfert d'argent national.
- Le logiciel MEI (Mandat express international) de transfert d'argent à international.
- Le logiciel Choice money logiciel de transfert d'argent à international et national.
- Le logiciel Orion de gestion des postes.
- Le logiciel CCM de gestion des comptes.
- Le logiciel IPS light
- Le logiciel CCB de gestion des comptes.
- Le logiciel Sage de comptabilité.
- Le logiciel Cyber café pro 3.5 et 5 de gestion du cyber café.

2.1.2 Les différents OS et logiciels utilisés

Les différents systèmes d'exploitation et logiciels utilisés sont :

Système d'exploitation	Logiciels
Windows XP, Windows 7, Windows 2008 et 2003 Server Standard et Entreprise,	Office 2007 et 2010, SAGE 1000 Antivirus Symantec, etc.

Tableau 4: les logiciels utilisés

L'ensemble des ressources informatiques de la société sont répartis, comme suit :

- Chaque direction dispose d'un dossier partagé des applications spécifiques et/ou non du service internet, auquel accède tout membre de la direction.
- Chaque division dans une direction dispose d'un dossier partagé où peut accéder tout membre de la division et auquel les membres des autres divisions de la direction ne peuvent pas accéder.
- Chaque section dans une division dispose d'un dossier partagé où peut accéder tout membre de la section et auquel les membres des autres sections de la division ne peuvent pas accéder.
- Chaque secrétariat de direction dispose d'un dossier partagé où peut accèder tout membre du secrétariat et le directeur. En plus, le secrétariat de la direction peut lire les rapports de chaque division, mais aucun des membres de la division n'accède au dossier du secrétariat.
- L'ensemble des directeurs de la SONAPOST et le Secrétaire Général disposent d'un dossier partagé où on peut accéder.
- Chaque membre d'une équipe (projet, section, division, direction, secrétariat) dispose de dossiers personnels, auquel aucune autre personne ne peut accéder.
- Les équipes de projet et les groupes de projet sont considérés respectivement comme des sections et des divisions.
- Les directions DFC et DSF n'ont pas droit au service internet.

MEHARI demeure l'une des méthodes d'analyse des risques les plus utilisées actuellement. Elle est dérivée de deux autres méthodes d'analyse des risques (MARION et MELISA). MEHARI est maintenue en France par le CLUSIF (Club de la Sécurité des Systèmes d'Information Français), via notamment le Groupe de Travail dédié à cette méthode.

MEHARI se présente comme une véritable boîte à outils de la sécurité des systèmes d'information. Elle permet d'appréhender le risque de différentes manières au sein d'une organisation et est composée de plusieurs modules qui, indépendamment de la démarche de sécurité choisie, permettent :

- d'analyser les enjeux de la sécurité (en décrivant les types de dysfonctionnements redoutés) et, corrélativement, de classifier les ressources et informations selon les trois critères de sécurité de base (Confidentialité, Intégrité, Disponibilité) ;
- d'auditer les services de sécurité de manière à prendre en compte l'efficacité de son contrôle et de synthétiser les vulnérabilités ;
- d'analyser les situations de risques permettant d'évaluer les potentialités et les impacts intrinsèques, ainsi que les facteurs d'atténuation de risque, puis, enfin, de déduire un indicateur de gravité de risque.

3.2.1 Description

Les utilisateurs pour avoir accès aux salles serveurs passent sous la surveillance d'un gardien et des caméras de vidéosurveillance. Les autres salles sont sous la

surveillance des agents de la société et des policiers dans certains centres à certaines heures.

3.2.2 La gestion du contrôle d'accès

La gestion du contrôle des accès physique est assurée par un gardien. Il est muni d'une autorité et décide des accès sur les directives du directeur de la Direction du Système d'Information. Au gardien s'ajoute le système de vidéosurveillance. Celui-ci permet de suivre les personnes ayant eu accès aux salles serveurs durant une période donnée.

3.2.3 Analyse critique

La gestion du contrôle d'accès physique assure la confidentialité, l'authenticité et la non-répudiation de l'usage des ressources par les utilisateurs. Cela constitue une force de grande importance dans le contrôle des accès aux ressources du système. En effet les accès aux salles n'étant autorisés qu'à un nombre limité de personnes et placés sous la vidéosurveillance, cela constitue une barrière solide.

3.3.1 Description

Les utilisateurs ont un accès direct aux ports de connexion du réseau. Ils peuvent ainsi se connecter au réseau avec n'importe quelle machine. Les machines sont connectées au réseau par configuration manuelle et accèdent au service réseau sans restriction d'accès.

3.3.2 La gestion du contrôle d'accès au réseau

Il n'existe pas de gestion de contrôle sur les accès de l'infrastructure réseau, sauf la connexion inter-sites VPN. Cette dernière est gérée par les serveurs VPN, qui offrent un contrôle sur les accès au système informatique de façon sécurisée. Les machines sont libres d'accès sur les réseaux sans contrôle d'accès quelconque, pourvu que leur configuration en IP leur permette une insertion dans un sous-réseau. Les entités sur le réseau ne sont pas identifiées lors de leur connection au système informatique.

3.3.3 Analyse critique

Force : suivant les prescriptions du contrôle d'accès en sécurité du système informatique, ce système offre une facilité d'accès rapide et une haute disponibilité à l'accès réseau.

Faiblesse : fort est de reconnaitre, une absence totale d'un contrôle d'accès (confidentialité, authenticité, intégrité et non répudiation). Cela constitue une faiblesse (un trou) de sécurité et expose le système à des attaques diverses. Un pirate peut accéder à l'infrastructure réseau en interne. Les attaques de tous les types pourraient s'en suivre, de sorte à paralyser le système et le rendre non fonctionnel. Comme attaque on pourrait citer :

- L'injection des vers et/ou des virus sur le réseau où certaines machines du réseau n'ayant pas d'anti-virus sont exposées à toutes sortes d'infections virales, surtout celles en provenance des vers et de cheval de Troie. En guise d'attention, 90% des travaux du service de Division Support et Systèmes (DSS), concernent la désinfection virale des machines conduisant, parfois à la réinstallation totale du système d'exploitation.

- Le vol d'information est rendu possible sur certaines machines fonctionnant sur du système Windows XP. En effet le compte Administrateur étant activé sans mot de passe et fréquemment utilisé comme compte utilisateur, les utilisateurs n'ayant aucune connaissance en sécurité informatique exposent ainsi les données du service sur le réseau.

- Les ouvertures extérieures dans certains services rendus possibles par l'usage de l'internet grâce aux clés de connexion des services de téléphonie mobile, alors que la politique de sécurité qui leur est assignée interdit l'usage de l'internet sur les postes.

- Les ouvertures logiques correspondant à des ports stratégiques restes ouverts sur certaines machines et des serveurs alors que pour des raisons de sécurité du système, ils devaient être fermés.

- L'absence d'une gestion centralisée des postes de service, ainsi que celle de la mise à jour des systèmes d'exploitation, des anti-virus et des logiciels fonctionnels est une véritable source de menaces aux systèmes d'information. En effet, les systèmes d'exploitation et les logiciels comportent des failles de sécurité dues à des erreurs de programmation ou de la non-prise en charge de certains paramètres de sécurité lors de l'implémentation. Ces failles sont exploitables par les pirates. Les mises à jour servent à

« boucher » ces trous de sécurité et d'avertir le système sur les nouvelles formes de menace. L'absence de ces mises à jour est une véritable source d'insécurité pour le système d'information et pour l'utilisateur en particulier. En somme, toute absence de mise à jour du système d'exploitation et de l'anti-virus expose les ressources du système et celles des utilisateurs (données personnelles) à la vue de la communauté des internautes. De plus, de nombreux virus et autres malwares profitent des failles de sécurité. Ces failles sont pour la plupart corrigées et le correctif est généralement proposé pour téléchargement sur le site web du producteur du système ou des anti-virus.

3.4.1 Description

Les utilisateurs, pour accéder aux ressources des machines et à celles du système d'information en général, s'authentifient (login et mot de passe d'un compte utilisateur) auprès du poste de travail où du domaine. Les utilisateurs pour la plupart ne possèdent pas d'identifiant dans le système. Le contrôle d'accès est ainsi effectué soit sur la machine locale, soit par le contrôleur de domaine suivant les comptes des ordinateurs et les comptes utilisateurs en local. Les postes de travail sont répartis en deux groupes selon le contrôle d'accès effectué :

- Les postes de travail libres sans attachement à un domaine sur lesquels il existe des comptes utilisateurs que tout utilisateur peut exploiter pour se connecter au système. Ils offrent un accès direct à ces ressources (puisque, ces comptes sont en majorité du groupe administrateur) et aux ressources partagées sur le réseau (fichiers, dossier, imprimante, application, logiciel, etc).

- Les postes de travail intègrent à un domaine, l'accès aux ressources de ces postes et aux autres ressources sont contrôlés par le contrôleur du domaine. Le contrôleur vérifie le compte utilisateur de la machine et lui accorde l'accès et les ressources partagées. Mais force est de constater que certains de ces comptes ne possèdent pas de mot de passe.

3.4.2 Gestion du contrôle d'accès

La gestion du contrôle d'accès logique au réseau est repartie sur cinq grandes catégories de dispositifs:

- Les domaines Windows qui sont au nombre de quatre (lapost.lan, sonapost.com, lapost.bf et sona-ips.lan) et répondent chacun à des projets de la SONAPOST. Chacun de ces domaines englobe des comptes utilisateurs et des ressources partagées (sur des applications ou des serveurs). Les contrôleurs des domaines veillent sur l'ensemble de leurs domaines pour assurer le contrôle total des accès et les droits des utilisateurs sur les ressources. Chaque domaine a son administrateur, sa politique administrative de sécurité et de contrôle d'accès.

- Les postes de travail libres ou les groupes (Workgroups) qui regroupent le reste des postes de travail et les serveurs auquels ils accèdent. Le contrôle est assuré par le système d'exploitation (dans sa politique de sécurité interne et la liste de contrôle d'accès sur les ressources) et les systèmes natifs des serveurs en gestion d'une ressource partagée.

- Le serveur des fichiers gère les fichiers partagés avec les listes des accès contrôlés (ACLs) et l'affiliation par groupe d'utilisateurs.

- Les serveurs d'applications protègent leurs ressources suivant des configurations de sécurité pour éviter les attaques de type injection de requête (SQL, XML, commande), parcours de répertoire, etc.

- Les imprimantes sont partagées suivant l'affiliation du poste administrateur de la machine à laquelle elles sont physiquement attachées.

3.4.3 Analyse critique

Force : cette diversité dans le contrôle d'accès et de sa gestion, rend le réseau hétérogène et confus face à une attaque organisée depuis l'extérieur. Les pirates ne pourront savoir quelles entités gèrent exactement les contrôles. De plus, l'isolement des forêts Windows sécurise toute infiltration depuis un réseau externe, sécurisant ainsi les ressources, qu'aux

utilisateurs définis dans celui-ci. Une haute disponibilité et une confidentialité sont assurées pour toutes les ressources à l'interne.

Faiblesse : Nous pouvons, au regard de tout cela, affirmer qu'il n'existe pas un domaine (système) propre à la SONAPOST. Ceux qui existent sont des projets informatiques, mais pas pour l'administration du système d'information de la SONAPOST. De ce constat, il advient qu'il n'existe pas de contrôle d'accès structuré selon une politique de sécurité. Il existe un amalgame de contrôle isolé et non structuré. Une multitude de systèmes de contrôle divers rendent totalement confuse la gestion du système. Cette multitude de systèmes de contrôle et de gestion est source d'insécurité. En effet, la multiplicité et la diversité des systèmes de contrôle d'accès liés aux contrôleurs des domaines et aux applications sont sources de contre-production. Chaque système (les domaines et les applications) est protégé par une procédure de contrôle d'accès spécifique. De ce fait, l'exploitation de chaque service nécessite un code d'authentification et des droits qui y sont associés. Cette multiplicité de contrôles d'accès est source de confusion pour les utilisateurs et les administrateurs qui, par exemple, perdent ou oublient leurs mots de passe.

D'une manière générale, du fait que chaque domaine et/ou application est géré par un administrateur unique, toute vision globale de l'ensemble des identités des utilisateurs et de leurs droits d'accès est impossible. Dans ce cas, l'administration autonome de chaque système est particulièrement source d'erreurs, de vulnérabilités et de perte de temps. Cette absence de vision globale sur l'ensemble des identités des utilisateurs et de leurs droits d'accès engendre des problèmes de responsabilité et d'information, une porte de vulnérabilité dans le système d'information. L'absence totale de la gestion centralisée des utilisateurs dans le système, fait que ces derniers doivent se débrouiller seuls : trouver le bon responsable pour l'accès à telle base de données, à telle application, à tel domaine, etc. Cela paralyse le système d'information et constitue une véritable menace à la sécurité de l'ensemble du système d'information, en particulier les ressources du système. Ce qui engendre des pertes et des dépenses financières en décrédibilisant la SONAPOST face à sa clientèle

Aussi, il est impossible pour les administrateurs d'être certains d'avoir supprimé tous les droits dont disposaient un employé partant ou d'avoir mis à jour les droits d'un employé

en cas de changement de fonction. Cela crée au sein du Système d'Information des comptes dits « fantômes » (dormants et/ou périmés) dans certains annuaires de domaine. De plus, les comptes techniques génériques, installés par défaut, par les systèmes d'exploitation et/ou les applications, ne sont pas toujours modifiés, voire supprimés, induisant d'autres failles de sécurité. Ceci étant d'autant plus grave que ces mots de passe sont facilement accessibles sur Internet. De même, certaines personnes utilisent, lorsqu'elles arrivent dans la société, des comptes utilisateurs « génériques » et partagés, simplement du fait de l'absence de création de leur propre compte.

Enfin, l'audit et la traçabilité sont les parents pauvres de la mise en œuvre des droits d'accès des utilisateurs. Pourtant, de plus en plus, la société doit respecter des normes, des lois et/ou des réglementations strictes en matière de politique de contrôle interne.

3.5.1 Description

L'utilisateur pour manipuler une ressource du système a besoin des droits que lui accorde le système.

- Les fichiers partagés résident sur des serveurs suivant l'organigramme de l'entreprise. Ainsi, suivant que l'utilisateur soit dans une direction, une division, une section ou une équipe, il peut accéder au répertoire du dossier partagé est associé. Il jouit ainsi de tous les droits (lire, écrire, créer, modifier, affichage de contenu), sauf celui du contrôle total.

- La plupart des applications de type web, sont hébergées sur des serveurs accessibles par tout utilisateur sur le réseau de la SONAPOST. L'unique contrôle d'accès effectué par ces applications est basé sur la liste des utilisateurs contenue dans leurs bases de données.

Les machines sont en elles-mêmes des ressources système. La connexion d'une machine à une autre ressource s'effectue, soit par appartenance à un sous-réseau (pour les imprimantes, les répertoires partagés) soit à un domaine (pour l'accès au logiciel logé dans le domaine). Autrement, toute connexion au serveur de fichiers et à celui des applications (logé dans un VLAN spécifique) est possible sur toute l'étendue du réseau.

3.5.2 La gestion du contrôle d'accès

D'une part, le contrôle d'accès est assuré par les ressources elles-mêmes (les applications possèdent en elles-mêmes cette fonctionnalité de contrôle –accès et une politique interne de sécurité). Cependant, l'usage le plus fréquent est celui des mots de passe et des login, gérés par les bases de données, qui évaluent l'exactitude des informations saisies. Il n'existe pas de politique de sécurité pour une relation générale de sécurité entre les applications. Ainsi, un employé peut évoluer de la caisse à l'inspection, puis au contrôle ou la réception principale et avoir toujours son compte (login et mot de passe de la caisse) dans la base de données de l'application de la caisse.

D'autre part, la gestion du contrôle est effectuée par les listes de contrôle d'accès, sur affiliation du groupe d'appartenance de la machine au domaine ou au groupe de travail. Le compte utilisateur est affilié au poste local. Ainsi, en fonction du poste local, l'utilisateur a accès à certaines données.

3.5.1 Analyse critique

Force : les moyens utilisés dans les applications limitent l'usage des ressources gérées par une application. Il en est de même pour les ACIs qui assurent une barrière infranchissable aux droits d'usage sur les fichiers et les répertoires.

Faiblesse : il s'agit là d'une force mal exploitée et non structurée. Ceci constitue une porte ouverte à une exploitation non judicieuse des fichiers et des ressources du logiciel, due à l'absence d'une politique bien définie des droits d'accès. Les ressources sont ainsi exposées aux erreurs de manipulation et à la malveillance dans leurs usagers. Ces derniers sont sources de défaillance du système d'information, et d'insécurité en matière d'intégrité, de confidentialité et de non répudiation.

En générale, nous percevons une absence de politique de contrôle d'accès sur infrastructure, une absence d'identification et de gestion centralisée des utilisateurs, des postes de travail et des autres ressources du système. A cela s'ajoute une absence de politique de gestion de la création des comptes, des mots de passe, des droits sur les ressources, des autorisations d'accès, du mode d'authentification et de surveillance sur l'ensemble des activités sur le système d'information.

De façon spécifique, les besoins en matière de contrôle d'accès aux ressources du système sont les suivants :

- Le contrôle d'accès au réseau en contrôlant :
    - l'accès des terminaux sur le réseau, suivant des critères bien définis ;
    - l'accès des périphériques réseau sur le média et les ports réseaux ;
    - la connexion des terminaux au système et les flux échangés;
- Le contrôle des droits d'accès aux ressources du système en contrôlant:
    - L'accès des utilisateurs du système, suivant des critères bien définis ;
    - Que chaque utilisateur accède aux ressources informatiques dont il a besoin pour l'accomplissement de sa fonction, suivant le principe du moindre privilège;

Conclusion

L'étude du système d'information nous a permis de découvrir l'environnement technologique, ainsi que la gestion des accès aux ressources système. A la suite de cette étude nous avons décelé le problème du contrôle d'accès aux ressources, ce qui nous conforte dans notre projet d'étude.

Il devient donc important pour nous, pour pallier ce problème d'avoir une vue globale sur le contrôle d'accès.

Introduction

Ce chapitre est consacré à l'étude du contrôle d'accès. Cette étude va nous permettre par la suite de mener à bien notre travail. Pour cela, nous allons commencer par une présentation de quelques concepts, suivie de celle des systèmes de contrôle d'accès actuels, pour finir avec une étude comparative et le choix d'un système de contrôle d'accès proposé à la SONAPOST.

1.1.1 Définition

Selon l'ISO 7498-2 : « Le service de contrôle d'accès assure une protection contre une utilisation non autorisée des ressources accessibles par une entité ou un groupe d'entités. Ce type de protection peut être appliqué pour différents types d'accès à une ressource ou pour tous les types d'accès. » Autrement dit, le contrôle d'accès peut se définir comme un mécanisme de limitation de l'utilisation d'une ressource (objet) aux seules entités (sujets) autorisées.

1.1.2 Objectif

Le contrôle d'accès fait partie des mécanismes de sécurité visant à protéger les ressources d'un système d'information. Nous entendons ici par ressource, tout composant (physique ou logique) participant à l'élaboration, au traitement, à la transmission, au stockage et à la destruction des données dans un système d'information. Comme de composants physiques, nous pouvons citer les serveurs, les points d'accès, les routeurs et comme composants logiques, nous avons les applications, les bases de données, les processus.

L'objectif du contrôle d'accès est de préserver la confidentialité, l'intégrité et la disponibilité des données et de fournir des preuves irréfutables sur l'usage des données par un utilisateur. De ce fait :

- La disponibilité d'un système d'information est le fait de rendre toutes les informations de ce système accessibles, à tout moment (par les acteurs ayant accès). Il est préférable que l'ensemble des données du système d'information soient disponibles rapidement.

- L'intégrité du système d'information a une importance capitale. Il s'agit ici de s'assurer que l'information est exacte, qu'elle n'a pas été altérée, ni modifiée. L'intégrité du système d'information doit être assurée pour les données elles-mêmes mais aussi pour le transit/traitement de ces données.

- La confidentialité consiste à s'assurer que l'information n'est accessible qu'aux seules entités ayant droits à telle ou telle information.

- La non-répudiation n'est pas un objectif en tant que tel. Elle est la garantie de pouvoir identifier à posteriori avec certitude les actions commises au sein du Système d'Information.

Le contrôle d'accès est une solution qui permet aux seuls utilisateurs autorisés d'accéder aux ressources du système d'information, tout en ayant vérifié au préalable qu'ils répondent aux critères établis pour y accéder. Il est le moyen le plus utilisé pour sécuriser les réseaux informatiques. Le contrôle d'accès assure les propriétés de sécurité (la confidentialité, l'intégrité et la disponibilité), il est aussi généralement capable de dicter à chaque utilisateur et administrateur son niveau d'accès une fois qu'il est sur le réseau.

Généralement, le contrôle d'accès se définit comme étant une implémentation des trois propriétés importantes de la fonction de sécurité des systèmes d'informations « les 3A » signifiant **a**uthentification, **a**utorisation, **f**acturation :

- Authentification : Cette première phase consiste à vérifier que l'utilisateur correspond bien à l'identité qui cherche à se connecter ;

- Autorisation : Cette phase consiste à vérifier que l'utilisateur, maintenant authentifié dispose des droits nécessaires pour accéder au système.

- Traçabilité (facturation) : Pour lutter contre les usurpations de droits, il est souhaitable de suivre les accès aux ressources informatiques sensibles (heure de connexion, suivi des actions, ...).

La figure 3 ci-dessous illustre le principe de fonctionnement du contrôle d'accès avec :

User : entités actives du système informatique, qui demandent des droits d'accès correspondant à l'autorisation d'exécuter des actions sur les objets. Ils incluent toujours les utilisateurs du système et aussi souvent les processus en cours d'exécution pour le compte des utilisateurs.

Security administrator : l'administrateur de la sécurité du système d'information.

System ressources : entités passives du système, qui contiennent les informations et ressources à protéger.

Authentication function : moyens permettant de certifie, la véracité de l'identité l'User.

Access control function : moyens permettant de certifie, les permissions de l'User sur les objets du systèm ressources.

Authentication : phase d'exécution de l'Authentication function.

Access control : phase d'exécution de l'Access control function.

Authorization database : moyens permettant au security administrator, d'accorder à l'User des permissions de manipulation des objets du systèm ressources.

Auditing : moyens permettant de suivre l'ensemble des activités au sien du système d'information.

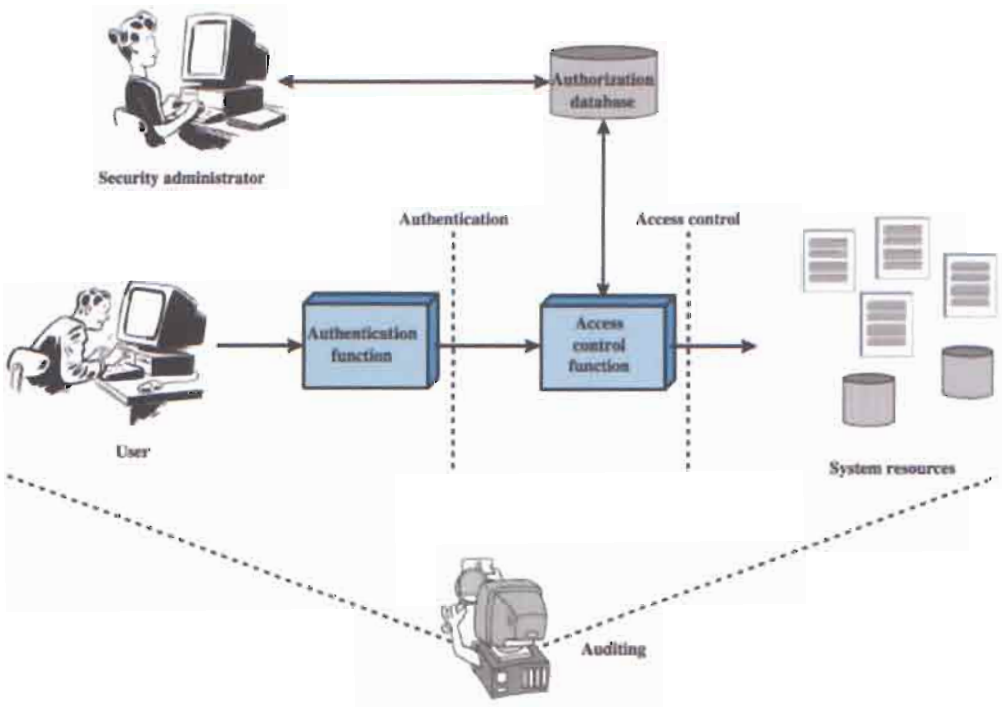


Figure 3 : Principe fonctionnel du contrôle d'accès

1.2.1 Politique de contrôle d'accès

Dans un système informatique, l'autorisation a pour but de ne permettre que les actions « légitimes », c'est-à-dire empêcher qu'un utilisateur puisse exécuter des opérations qui ne lui sont pas permises. Pour définir quelles sont les opérations autorisées et celles qui sont interdites, il faut établir une politique de contrôle d'accès. Le standard européen ITSEC (Information Technology Security Evaluation Criteria) définit une politique de sécurité comme étant « l'ensemble des lois, règles et pratiques qui régissent la façon dont l'information sensible et les autres ressources sont gérées, protégées et distribuées à l'intérieur d'un système spécifique ». Les politiques de contrôle d'accès peuvent être groupées en trois principales classes :

- les politiques discrétionnaires (DAC) qui accordent au propriétaire de l'information, généralement le créateur, tous les droits d'accès ainsi que la possibilité de les propager aux autres selon sa discrétion;

- les politiques obligatoires (PHYSIQUE) qui décrètent des règles incontournables régissant les droits des sujets et des objets. Elles permettent de restreindre les privilèges que possèdent les sujets sur les objets qui leur appartiennent ;

- les politiques basées sur les rôles (RBAC) qui sont les plus récentes servant à décrire d'une manière plus expressive et plus puissante les fonctionnalités dans les organisations. Les droits d'accès sont accordés aux rôles, et aux tâches dans l'organisation. Ils sont attribués aux sujets en fonction des rôles qu'ils jouent.

1.2.2 Types de contrôle d'accès

On distingue trois types de contrôle d'accès à savoir: le contrôle d'accès administratif, le contrôle d'accès technique, le contrôle d'accès physique.

- **Le contrôle d'accès administratif** est opéré à travers des documents décrivant les politiques, les rôles et responsabilités, et les fonctions administratives nécessaires pour gérer l'environnement de contrôle. Il définit un ensemble de procédures et de moyens qui traitent de tout ce qui ressort de la sécurité, d'un point de vue organisationnel, au sein de l'entreprise. La structure de l'organigramme ainsi que la production des applicatifs en font partie. Les propriétés de sécurité recherchées visent, par exemple, à limiter les cumuls ou les délégations abusives de pouvoir, ou à garantir une séparation des pouvoirs.
- **Le contrôle d'accès technique** concerne tous les accès logiques aux ressources du système d'information. Il est implémenté avec des solutions logicielles et matérielles s'appuyant sur des technologies.
- **Le contrôle d'accès physique** concerne tous les accès physiques aux locaux et ressources matérielles. Il précise un ensemble de procédures et de moyens qui protègent les locaux et les biens contre les accès physiques aux matériels informatiques et de communication (gardiens, codes, badges, ...).

Les systèmes de contrôle d'accès sont classifiés suivant les types de contrôle d'accès définis ci-dessus. Dans notre cas, seuls les systèmes de contrôle d'accès technique (logique) recevront notre intérêt dans la réalisation de notre projet. Il s'agit des systèmes de contrôle d'accès à l'infrastructure et aux ressources du système. Les systèmes de contrôle d'accès logique sont souvent répartis en trois catégories : les systèmes de filtrage, les systèmes d'authentification et les systèmes de chiffrement des liaisons (cryptage de données circulant sur le réseau).

2.1 Le système de contrôle d'accès par filtrage (Firewall)

Les pare-feu peuvent aussi agir en tant que passerelles de réseaux privés virtuels. Ces dispositifs permettent le filtrage de l'accès au réseau interne, comme illustre dans la figure 4, afin d'empêcher l'accès non autorisé à l'ensemble des services du réseau. Il s'agit de contrôler les flux entrant sur le réseau. Plusieurs types de filtrage sont proposés :

- le filtrage applicatif pour le contrôle des applications en fonction du port utilisé ;
- le filtrage utilisateur pour le contrôle d'accès en fonction des utilisateurs identifiés ;
- le filtrage adaptatif permettant l'émission d'un journal des transmissions de paquets IP.

La configuration d'un filtre s'effectue généralement au travers de liste de contrôle d'accès (Access Control List ou ACL), constitué par la mise bout à bout des différentes règles à suivre. Cette liste est lue séquentiellement jusqu'à la dernière règle applicable qui est retenue.

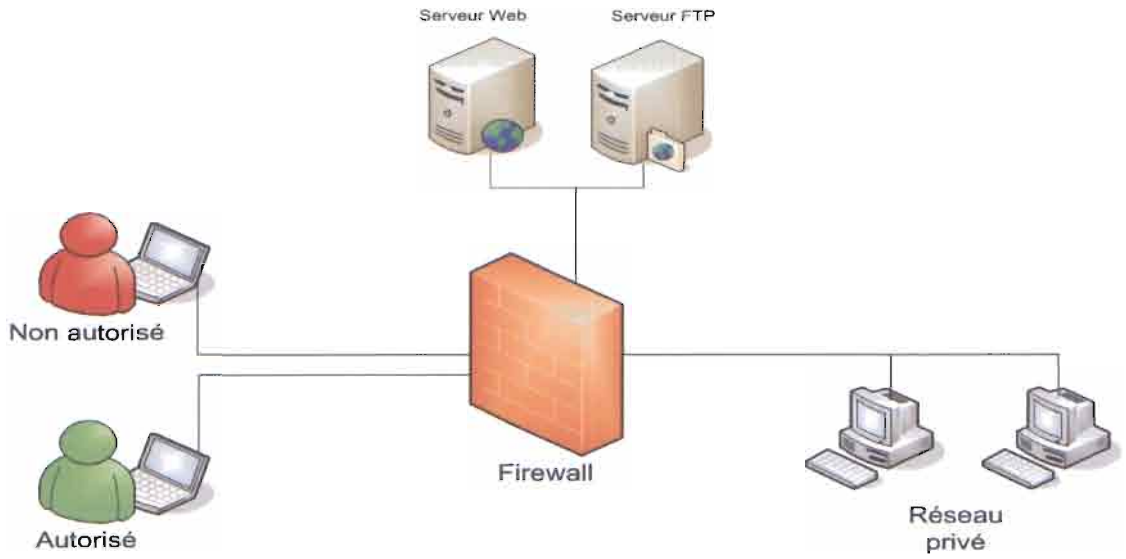


Figure 4 : Représentation d'un système de filtrage

2.2 Le système de contrôle d'accès par authentification et autorisation

L'authentification est un mécanisme qui permet de prouver l'identité dont se réclame une entité (utilisateur, application, équipement...) ayant à interagir avec les autres objets du système d'information. Le système d'authentification consiste à vérifier l'authenticité et les

autorisations des utilisateurs et des périphériques informatiques qui accèdent à des zones privées du système d'information. Il fait référence à un mécanisme de sécurité, lequel repose sur un triple service d'identification, d'authentification et d'autorisation, avec la fonctionnalité de journalisation des activités. Ainsi, avant toute utilisation des services du système, l'accédant devra décliner son identité (identification) et prouver qu'il est bien celui qu'il prétend être (authentification). Une fois la relation établie, les actions légitimes qu'il peut accomplir sont déterminées par la politique d'autorisation. L'authentification peut se faire de multiples manières, et notamment par la vérification de l'adresse physique de la carte Ethernet, de login/mot de passe (windows, LDAP...), de certificats (utilisateurs ou machines), une carte à puce, une caractéristique propre de l'accédant, etc.

Ce moyen peut être utilisé pour le contrôle d'accès logique. L'information chiffrée transmise peut être seulement décodée et accessible seulement par les utilisateurs qui possèdent la clé adéquate. Ceci est particulièrement utile en l'absence de contrôles d'accès physiques rigoureux. C'est le cas pour les ordinateurs portables ou pour les supports de données comme les clés USB ou disques durs externes. Il s'agit de protéger les données contenues sur ces matériels afin qu'elles ne soient pas accessibles que par la personne autorisée et pas par l'auteur du vol du matériel.

Le tableau 4 suivant compare les aspects des systèmes de contrôle d'accès près-cités.

Tableau 5 : Comparaison des systèmes de contrôle d'accès

	Filtrage	Authentification	Cryptage/Chiffrage
Identification de l'utilisateur	Non	Oui	Oui
Identification de la machine	Oui	Oui	Oui
Protection contre l'usurpation d'identité	Non	Oui	Oui
Niveaux de couche de protection (OSI)	2 à 7	2, 3,7	2,3 ,7
Interaction avec les autres	Non	Oui	Non
Coût de mise en œuvre	faible	élevé	très élevé

L'authentification est un mécanisme de sécurité qui consiste à assurer l'identité d'un utilisateur, ou d'une machine voulant accéder au système. Ainsi, nous vérifions que la station ou la personne, est bien celle qu'elle prétend être. Ce mécanisme pose tout de même certains problèmes. Par exemple, lorsqu'un utilisateur a besoin de se connecter sur plusieurs stations différentes, le mécanisme devient relativement lourd. Ce mécanisme d'authentification permettant un niveau de sécurité élevé, est celui qui fait appel à un serveur d'authentification, qui centralise, géré et contrôle tous les accès aux ressources du système, c'est ce mécanisme que nous allons implémenter dans notre travail.

Conclusion

Au terme de ce chapitre, il faut retenir que pour mieux comprendre notre projet, une étude générale du contrôle d'accès et de quelques systèmes de contrôle d'accès était nécessaire. En effet, ce chapitre nous a permis d'avoir un aperçu sur les exigences en contrôle d'accès et de porter une analyse sur les systèmes de contrôle d'accès, afin de faire des choix judicieux pour la sécurité de notre système d'information.

Dans le chapitre qui suit, nous allons passer à l'étude conceptuelle de la solution de contrôle d'accès proposée et en sa mise en place au sein du système d'information de la SONAPOST.

Introduction

Dans ce chapitre, nous présentons l'architecture du futur système de contrôle d'accès et son déploiement au sein du système informatique de la SONAPOST. Une maquette du modèle de déploiement sera présentée suivant les choix stratégiques de sécurité et la planification de la mise en œuvre, pour finir avec le bilan et les perspectives.

La topologie physique du système est en étoile hiérarchique à trois couches de nœud, avec comme nœud centrale l'annuaire, le nœud secondaire l'ensemble des serveurs d'authentification et les proxys RADIUS et le troisième nœud les systèmes authentificateurs. Ces derniers centralisent les VLAN des différentes entités sur le réseau et les groupes d'utilisateurs sur les systèmes d'exploitation et système de fichiers. L'architecture logique du futur système d'information est représentée, par une répartition des différentes entités du réseau en des VLAN et les utilisateurs en des groupes dits « groupe de sécurité », cela en conformité avec les objectifs techniques définis.

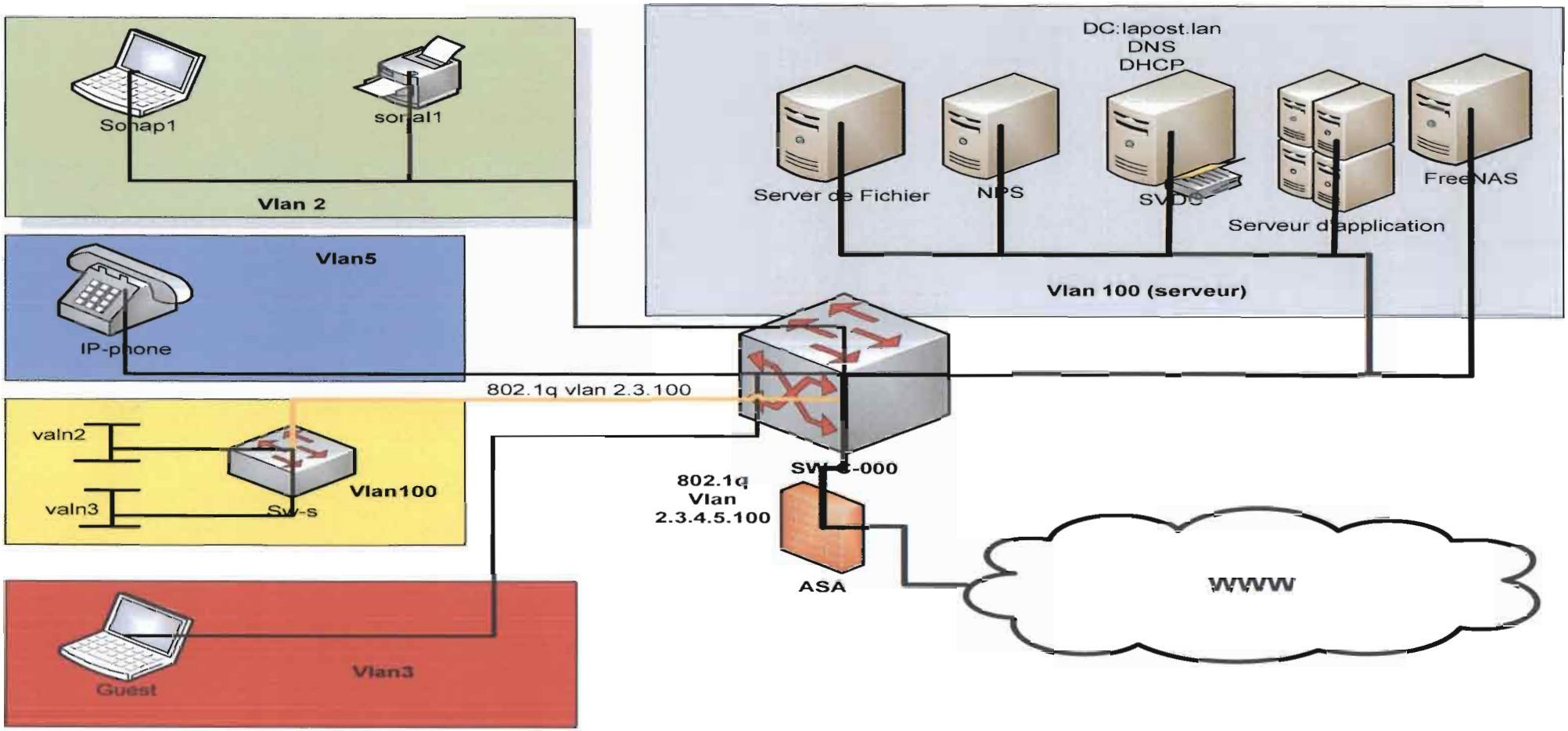


Figure 5 : Schéma de l'architecture du système

Le nouveau système de contrôle d'accès est basé sur le système d'authentification et autorisation, qu'offrent les serveurs d'authentification en interaction avec des systèmes authentificateurs et le service annuaire. L'annuaire fournit l'ensemble des identités et l'autorisation liée à chaque identité au serveur d'authentification pour la vérification des droits d'accès et des différentes entités aux ressources. Les serveurs d'authentification appliquent les droits d'accès via les systèmes authentificateurs, qui sont chargés de veiller à ce que tous ceux qui accèdent à une ressource aient été authentifiés et n'exercent que ses droits sur cette dernière. Le serveur d'authentification authentifie et autorise les tentatives d'accès à une ressource et journalise l'ensemble des transactions qu'il traite. Couplé à des serveurs proxy RADIUS et aux contrôleurs de domaine secondaire des sites, il fournit un service de contrôle d'accès centralisé et distribué au sein du réseau WAN de la SONAPOST.

2.1.1 Les technologies d'authentification

Déployer des technologies de sécurité réseau pour protéger l'intranet contre des hôtes inconnus doit se faire en fonction du niveau de sécurité souhaité, du prix et de la facilité de déploiement. Les hôtes inconnus sont des ordinateurs qui ne font pas partie de l'infrastructure de sécurité ou de gestion de l'intranet, tel que le service d'annuaire Active Directory. Nous détaillons ci-après le fonctionnement des trois solutions majeures d'authentification.

- **Authentification WEB-based**

L'authentification par le biais d'un navigateur internet est certainement la plus simple à mettre en œuvre. Ce type d'authentification est largement utilisé dans les

espaces « libre-service » afin que les clients extérieurs puissent avoir accès au réseau sans avoir à paramétrer leur système. La méthode d'authentification s'effectue par le biais d'un navigateur internet sur lequel le client réseau est invité à saisir un nom d'utilisateur et un mot de passe. Lorsque l'authentification est validée, le trafic réseau du client peut circuler sur le réseau interne. Deux formes d'authentifications « Web » existent : le « Web-Based» intégré au NAS et le portail captif. Ces deux solutions présentent des avantages quasiment identiques, mais celle réalisée via un portail captif autonome reste plus souple quant à sa mise en œuvre et à sa configuration. Il est à noter que pour cette solution, il est nécessaire de prendre en compte l'expiration du bail de l'adresse IP du client réseau si celui-ci doit être redirigé sur un autre VLAN avec une adresse IP différente.

- **Authentification PHYSIQUE-BASED**

Ce mode d'authentification permet de rendre très souple la configuration des points d'accès, car la procédure de contrôle est fondée sur l'adresse physique (PHYSIQUE) du client réseau. Ce mode de contrôle des clients n'est pas le plus sécurisé, mais offre une certaine facilité de mise en œuvre dans un environnement existant. Dans ce cas, l'adresse PHYSIQUE servira d'identifiant de référence pour l'authentification sur le RADIUS. En cas de succès ou d'échec de l'authentification, les attributs-valeurs permettent d'orienter le client vers un VLAN prédéfini.

Nous considérons que l'authentification par adresse PHYSIQUE convient parfaitement aux clients qui ne peuvent fournir d'authentifications interactives telles que les téléphones IP, les imprimantes, les postes nomades, etc. En raison du nombre de clients potentiels, l'utilisation d'une base de données pour l'authentification est particulièrement conseillée.

- **Authentification en 802.1X**

Ce mode d'authentification diffère des deux solutions précédentes en ce qu'il nécessite la mise en place d'une Infrastructure de Gestion de Clefs (serveur PKI). Cette méthode requiert la création de certificats qui permettront d'authentifier les clients de manière unique. Un certificat dit "client" est installé sur le client réseau. Lors de la connexion, seuls sont autorisés les échanges relatifs à la validation du certificat.

Après validation de ce dernier par le serveur RADIUS, le client est autorisé à se connecter, sous réserve des restrictions d'accès qui peuvent lui être imposées lors de la phase d'échange des autorisations entre le point d'accès et le RADIUS.

2.1.2 Choix de la technologie d'authentification

Après avoir présenté les trois grandes solutions d'authentification et de contrôle d'accès et sachant qu'il est possible à tout moment de connaître la localisation d'un client sur le réseau, nous pouvons désormais proposer une solution de contrôle d'accès des postes clients, fondée sur la norme 802.1x. Du point de vue de la sécurité, il est préférable de déployer des technologies de sécurité pour fournir une défense en profondeur afin de créer plusieurs barrières face à un attaquant. Le déploiement de 802.1X pour les réseaux filaires permet d'empêcher des hôtes inconnus d'accéder à votre intranet. Pour nous conformer aux objectifs de notre projet, nous avons adopté le déploiement de 802.1x pour les réseaux filaires.

2.2 [illegible]

2.2.1 Les serveurs d'authentification

Un serveur d'authentification et d'autorisation est l'élément chargé de gérer le processus de communication entre lui et le client. Il permet au client de s'authentifier et d'accéder ou non aux services réseaux demandés. On distingue plusieurs serveurs d'authentification et d'autorisation dont les plus connus sont de type RADIUS. Nous disposons des serveurs suivants :

- **NPS de Windows Server 2008 R2**:

NPS, ou Network Policy server, est l'un des rôles disponibles sur Windows 2008 server. Il est le remplaçant d'IAS (Internet Authentication Service) disponible sur Windows 2003 Server. Au même titre qu'un serveur RADIUS, NPS gère l'authentification et les autorisations selon les différents modes de connexion (locale, VPN...).Il permet entre autre :

- l'accès aux ressources locales via une connexion à distance (VPN...) ;

- authentification via Active Directory ;
- gestion des droits via GPO.

- **Free RADIUS** :

Free RADIUS est une implémentation de RADIUS élaborée, à la suite du projet Cistron, par un groupe de développeurs. La scission entre les deux projets date de 1999. C'est un projet Open Source sous licence GPL.

- **Cisco Secure ACS:**

Le serveur de contrôle d'accès Cisco Secure ACS (Access Control Server) pour Windows 2000 est l'une des nombreuses solutions logicielles de sécurité proposées dans la suite Cisco. Il permet l'authentification, l'autorisation et la gestion du trafic et des utilisateurs. Ce service est aussi appelé AAA (Authentication, Authorization, and Accounting). Cisco Secure ACS pour Windows 2000 facilite l'application de services AAA à tous les environnements d'accès, petits et grands. Ce service parfaitement intégré à Windows 2000 facilite le déploiement et la mise en œuvre de différents services, tels que l'accès à distance des réseaux privés virtuels (VPN), le contrôle de l'accès selon l'heure et divers degrés possibles de communications sécurisées. Cisco Secure ACS convient à la mise en place initiale d'un système de sécurité et peut ultérieurement être mis à jour pour prendre en compte des environnements plus complexes et l'évolution des politiques de sécurité.

2.2.2 Choix du serveur d'authentification et d'autorisation

Pour pouvoir choisir efficacement les différentes solutions qui s'offrent à nous en termes de serveur pour implémenter le contrôle d'accès 802.1X, il nous faut définir des critères d'évaluation qui détermineront la valeur du produit. Nous avons (très bon : 3 ; bon : 2 ; moyen : 1 faible : 0)

Tableau 6 : Comparaison des serveurs RADIUS

	Windows Server 2008 R2	Cisco Secure ACS	Free RADIUS
Note du Prix	Bon	Moyen	Très bon
Note de Qualité	Très bon	Très bon	Bon
Note de Solidité	Très bon	Bon	Moyen
Note du Support	Moyen	Moyen	Bon
Note Documentation	Très bon	Très bon	Moyen
Note de Facilité	Très bon	Très bon	Faible
Note de Suivi	Bon	Bon	Très bon
Note d'intégration	Très bon	Moyen	Moyen
Score sur 24	**20**	**15**	**13**

Nous trouvons que la solution Windows Server 2008 R2 est la plus efficace et utile en terme d'implémentation du protocole 802.1x. L'utilisation de 802.1X, avec Windows Server 2008 R2 côté serveur et Windows du côté des clients, est idéale pour se prémunir des dangers d'une machine inconnue et dont l'état de santé est mauvais et potentiellement malveillante. Son prix reste raisonnable comparé aux couts d'irnplémentations d'autres grands constructeurs. Windows Server 2008 R2 a aussi l'avantage d'offrir de multiples fonctionnalités en plus. Il fait tout en un et c'est un avantage non négligeable.

Ce choix ne signifie pas que les autres solutions n'ont pas de mérite, mais simplement qu'avec un budget raisonnable et un effort raisonnable on parvient rapidement à des résultats probants et efficaces.

3.1.1 Concept de groupe d'objets

La politique, où les droits d'accès sont attribués à l'utilisateur en fonction du rôle qu'il joue dans le système d'information, est appelée politique par rôle. Le rôle désigne une entité intermédiaire entre utilisateurs et privilèges (ensembles de droits). Les rôles permettent de faciliter l'administration de la politique de sécurité et de réduire les coûts de gestion des droits d'accès. Les privilèges seront attribués seulement selon le rôle en respectant :

- la relation professionnelle existante entre les services, les divisions et les directions;
- l'implication professionnelle dans le processus de traitement des dossiers (projet, rapport, etc.) ;
- d'autres informations contextuelles comme le lieu, le temps, la promotion, l'urgence, la permutation, etc.

C'est dans cette logique et afin d'offrir un contrôle d'accès plus adapté, que nous introduisons le concept de groupe d'objets.

Nous partitionnons l'ensemble des éléments du système en deux grandes catégories:

- les *sujets* sont des entités actives (utilisateurs) qui manipulent l'information,
- les *objets* sont des entités passives (fichiers, application, imprimante, etc.), contenant de l'information, sur lesquelles les sujets effectuent des actions.

Par spécification, nous identifions des classes d'objets: équipements, dossiers, etc. Néanmoins, du point de vue du contrôle d'accès, cette classification est insuffisante et il nous faudra distinguer les objets passifs de la même classe, sur lesquels les sujets peuvent avoir des droits différents; d'où l'idée de construire des groupes d'objets selon des critères liés aux droits d'accès.

La construction des groupes d'objets se fait en trois étapes:

- **Première étape**: selon une vue *logique*,

Le regroupement d'objets (dossiers traités par un agent, par une division et par groupe de projet et les ressources d'un agent, un groupe, une division/ direction) ce fait par rassemblement des objets sur lesquels un groupe de sujet effectue une même actions.

- **Deuxième étape**:

Relier chaque groupe avec les actions effectuées sur les objets qui le constituent. La manière utilisée est le regroupement des objets sur lesquels sont effectuées les mêmes actions. Ainsi, en jouant un rôle donné, l'utilisateur obtient des privilèges lui permettant de réaliser des actions, non pas sur tous les objets d'une classe, mais sur une partie désignée par le groupe mentionné.

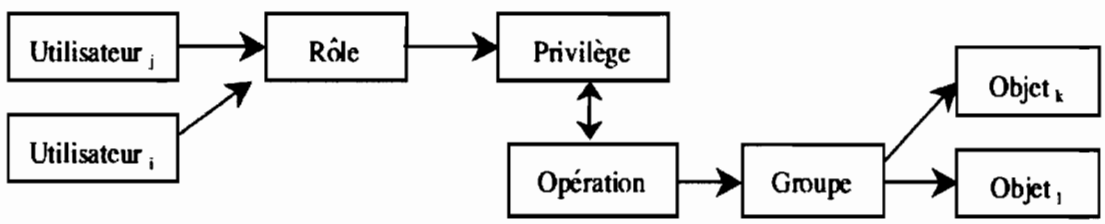


Figure 6 : Conception de groupe

❖ **Troisième étape** :

Réduire la complexité et améliorer la structuration à travers l'héritage de classes d'objets ou la composition de groupes d'objets.

3.1.2 Méthode d'autorisation

Dans la pratique de ce concept de groupe d'objets, nous utiliserons la stratégie **A G DL P** des groupes de sécurité pour la gestion des accès aux ressources. Nous en définissons deux catégories de groupe suivant les étendues de groupe. Le GPO sera utilisé pour l'application des stratégies de la politique de sécurité dans les groupes de sécurité.

Un bon usage de ces groupes nous permet d'arriver à nos objectifs. L'une des stratégies d'usage de ces étendues de groupe est la stratégie **A G DL P.** Le principe de la stratégie A G DL P est le suivant : ajouter des comptes d'utilisateur (**A**) dans des

groupes globaux (**G**), placer les groupes globaux dans des groupes de domaine local (**DL**), puis accorder des autorisations (**P**) au groupe de domaine local.

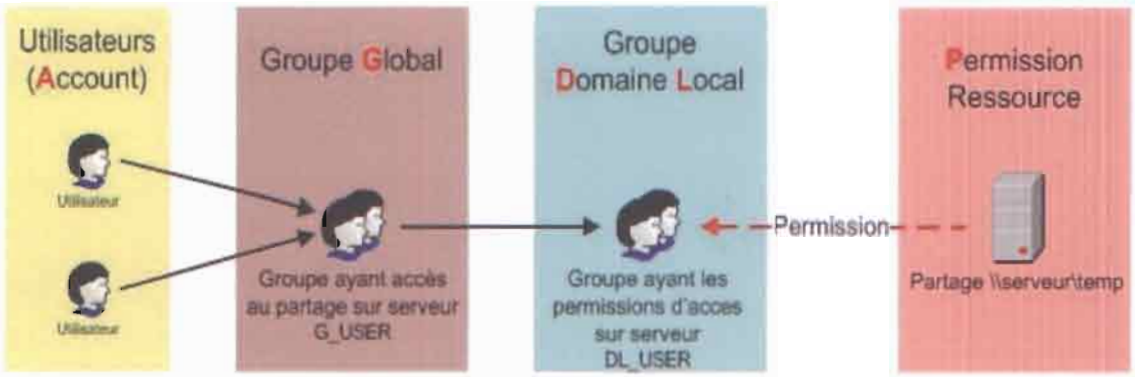


Figure 7 : Représentation de la stratégie AGDLP

3.1.3 Le gestionnaire des identités et des habilitations

Le gestionnaire des identités et des habilitations, est assuré par l'annuaire Active Directory de la SONAPOST. L'active Directory est la base de données des objets tels que les utilisateurs et les équipements réseau de notre système d'information. C'est sur cette base de données que les contrôleurs d'accès vont s'appuyer pour identifier les suppliants qui sont autorisés à accéder aux ressources du système d'information.

L'ensemble des attributions, des habilitations, des équipements réseau et des utilisateurs est défini par leurs rôles au sein du système d'information. Ces habilitations sont représentées par leur appartenance à un groupe défini, dont le système lui reconnait certains droits d'accès.

Nous définissons ainsi avec le modèle des groupes, cinq types de groupes de caractère d'identification, qui permettra d'authentifier qu'un utilisateur ou un équipement réseau est de la société.

- Le groupe ordinateur regroupe l'ensemble des ordinateurs de la société ;
- Le groupe imprimante regroupe l'ensemble des imprimantes de la société ;
- Le groupe téléphone IP regroupe l'ensemble des téléphones de la société ;
- Le groupe switch et hub regroupe l'ensemble des switch et hub de la société ;

- Le groupe Utilisateur regroupe l'ensemble du personnel de la société.

L'ensemble de ces groupes est affecté à quatre catégories groupes, sur lesquels s'appliquent les stratégies de politique de sécurité de contrôle d'accès.

- Le Groupe_802.1x : contient tous les équipements réseau sur lesquels s'applique le contrôle d'accès réseau par la norme 802.1x;
- Le Groupe_nap : contient tous les ordinateurs sur lesquels s'applique le contrôle sanitaire par NPS;
- Le Groupe_DG : contient l'ensemble des ordinateurs de la Direction Générale ;
- Le Groupe_DSI : contient l'ensemble des ordinateurs de la Direction des Systèmes d'Informations;
- Le Groupe_DFC : contient l'ensemble des ordinateurs de la Direction Financière et Comptable;
- Le Groupe_DC : contient l'ensemble des ordinateurs de la Direction du Courrier ;
- Le Groupe_DSF: contient l'ensemble des ordinateurs de la Direction des Services Financiers ;
- Le Groupe_DRH : contient l'ensemble des ordinateurs de la Direction des Ressources Humaines ;
- Le Groupe_DFC : contient l'ensemble des ordinateurs de la Direction du Patrimoine et de la Logistique ;
- Le Groupe_DCM : contient l'ensemble des ordinateurs de la Direction Commerciale et Marketing ;
- Le Groupe « rôle »: contient tous les utilisateurs sur lesquels s'appliquent les privilèges de contrôle d'accès aux services partagés et aux ressources;
- Le Groupe « privilège »: contient tous les utilisateurs et groupe sur lesquels s'applique, le contrôle d'accès aux services partagés et aux ressources.

3.2 Le système authentificateur du 802.1x

3.2.1 Instances

Le système authentificateur est assuré par les switchs du réseau implémentent 802.1x.

Dans ce projet, nous pouvons identifier différentes instances :

- L'instance Intern qui sera dédiée aux postes de la société;
- L'instance Voice qui sera dédiée aux téléphones IP de la société ;
- L'instance Print qui sera dédiée aux imprimantes de la société ;
- L'instance Network qui sera dédiée aux équipements réseau validés ;
- L'instance Guest qui sera réservée aux postes externes de la société.

3.2.2 Conception des méthodes d'authentification

- **L'Instance Intern**

L'accès à cette instance qui donne accès au VLAN permettant l'utilisation des ressources de la société (Serveurs de fichier, imprimantes, etc...), sera contrôlé par la méthode d'authentification EAP-TLS en combinaison d'un certificat côté serveur et côté client. Nous voulons authentifier les postes de la société de façon automatique et transparente sans que l'utilisateur ait à fournir un nom d'utilisateur et un mot de passe.

Les certificats garantissent l'identité du « supplicant » et du serveur d'authentification afin de pouvoir créer un tunnel sécurisé TLS pour chiffrer leurs échanges d'informations. La figure 8 illustre le fonctionnement de EAP-TLS.

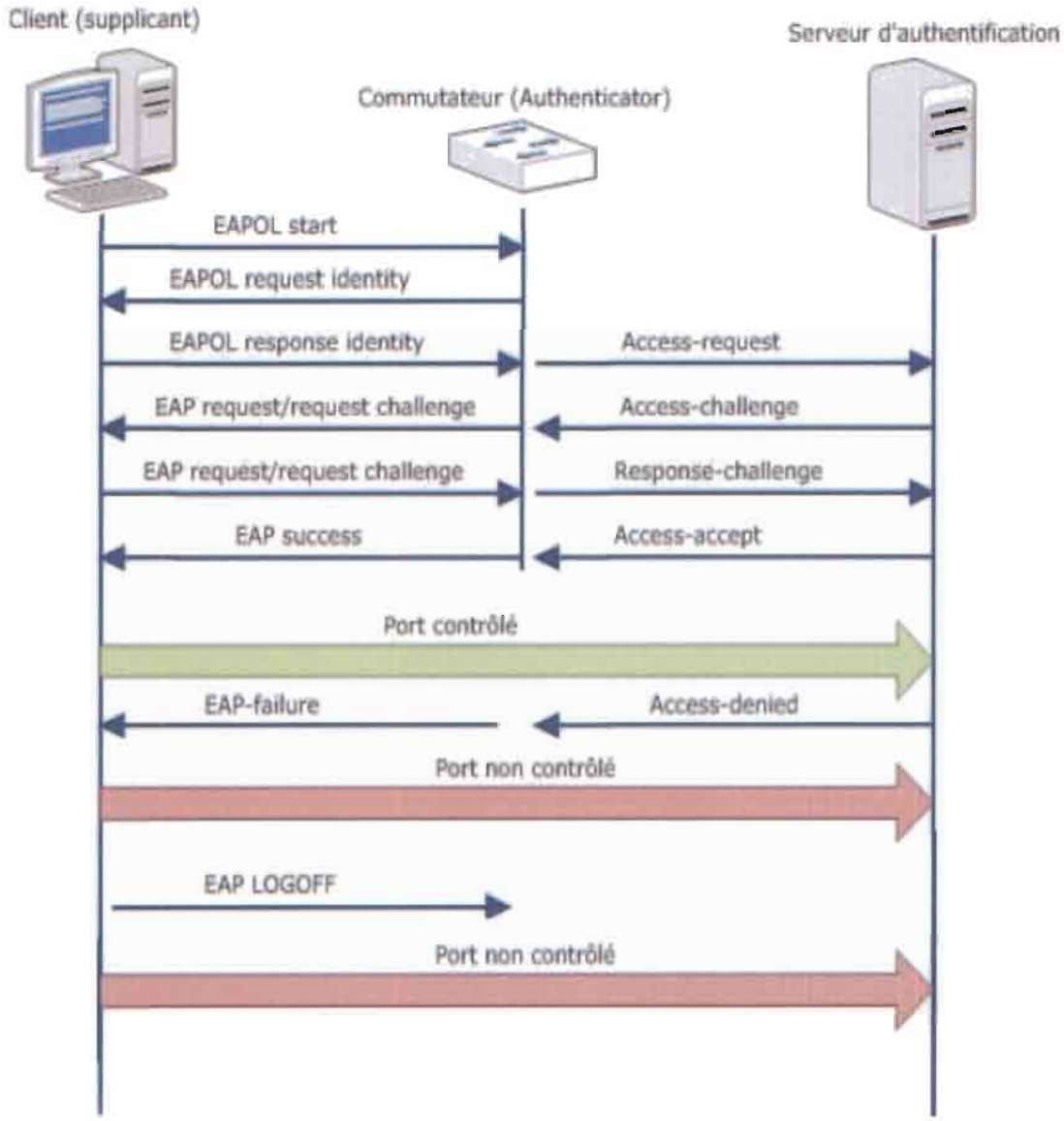


Figure 8 : Echange d'informations lors du processus EAP-TLS

- **L'instance Voice**

Cette instance donne accès au VLAN permettant de véhiculer les trames de voix au central téléphonique IP (pas disponible pour ce projet). Pour cette instance, on peut identifier une problématique : selon les besoins exprimés, les téléphones IP de l'entreprise doivent être acceptés par défaut. Pour ce faire, il existe plusieurs solutions pour vérifier qu'ils appartiennent bel et bien à la société :

- **L'authentification du téléphone par 802.1x.**

Cela n'est pas très pratique car il est nécessaire que le téléphone soit compatible avec la norme 802.1x. Il faut également saisir un nom

d'utilisateur et un mot de passe sur le téléphone lorsqu'on le connecte sur le réseau.

- **La configuration d'une exception de l'adresse physique du téléphone, configurée directement sur le port du Switch.**

  Cette configuration n'est pas très pratique pour l'administration car il faut configurer le Switch à chaque fois qu'on ajoute ou qu'on enlève un nouveau téléphone. Avec plusieurs Switches, les adresses physique ne seront pas centralisées.

- **Configuration d'une « exception » de l'adresse physique (MAB - Physique Adress Bypass) configurée sur le Switch. La base de données des adresses physique autorisées se trouverait directement dans une Policy RADIUS.**

  Le champ texte utilisé à cet effet est limité à 256 caractères donc si on a plusieurs téléphones, il y a un risque de n'avoir pas assez de place et il faut donc créer plusieurs policies.

- **Configuration d'un « Bypass » sur l'adresse physique (MAB) configurée sur le Switch. La base de données des adresses physique autorisées se trouverait dans un service d'annuaire (tel qu'Active Directory) sous forme de « users » dans une unité organisationnelle et un groupe de sécurité.**

  Pour notre projet, nous jugeons que la dernière solution serait la plus adéquate pour pouvoir gérer les adresses physique de façon centralisée.

Le but de MAB est d'authentifier le suppliant quand l'authentification EAP échoue et ainsi d'envoyer comme nom d'utilisateur et comme mot de passe l'adresse PHYSIQUE du suppliant au RADIUS.

- **L'Instance Print**

Cette instance sera placée dans le même VLAN que les ordinateurs de l'entreprise. Toutefois, la définition d'une instance séparée est nécessaire puisque l'analyse des besoins nous indique que les imprimantes de la société doivent être

acceptées par défaut. Par conséquent, elles ont besoin d'un autre « traitement » d'authentification que les ordinateurs.

Nous pouvons donc observer la même problématique que pour l'instance Voice et nous avons par conséquent opté pour la dernière solution.

Cette solution prévoit l'activation du MAB sur le port 802.1x du Switch pouvant gérer les exceptions des adresses physiques.

Comme pour l'instance Voice, les adresses physiques des imprimantes autorisées seront placées dans un service d'annuaire sur lequel se basera le service RADIUS pour appliquer l'exception.

- **Instance Network**

Cette instance est prévue pour pouvoir cascader un Switch validé 802.1x avec un Switch authentificateur 802.1x. Ceci peut être nécessaire si on veut rendre disponibles plus de ports dans un bureau pour une utilisation spécifique (c'est-à-dire accès à un VLAN spécifique).

L'instance network peut authentifier uniquement des Switches de gamme professionnelle (tels que les Switch Cisco ou 3com) compatibles 802.1x. De cette manière le Switch d'extension sera authentifié par le Switch authentificateur en utilisant le même principe que pour l'instance Print c'est-à-dire avec le MAB.

- **Instance Guest**

L'instance Guest donne accès uniquement à internet. Elle est complètement isolée des autres instances et est prévue pour tous les autres périphériques Ethernet.Ce qui inclut des Switch de la gamme non professionnelle et non compatible 802.1x.

L'accès à cette instance ne sera pas contrôlé par le serveur RADIUS mais par le Switch même. Quand les deux méthodes d'authentification 802.1x (MAB et dot1x) échouent, le Switch met le périphérique automatiquement dans le VLAN Guest.

3.2.3 Illustration du concept et de la solution choisie

Le principe de contrôle d'accès de quels équipements accèdent à certains ressources est illustré au figure 9.

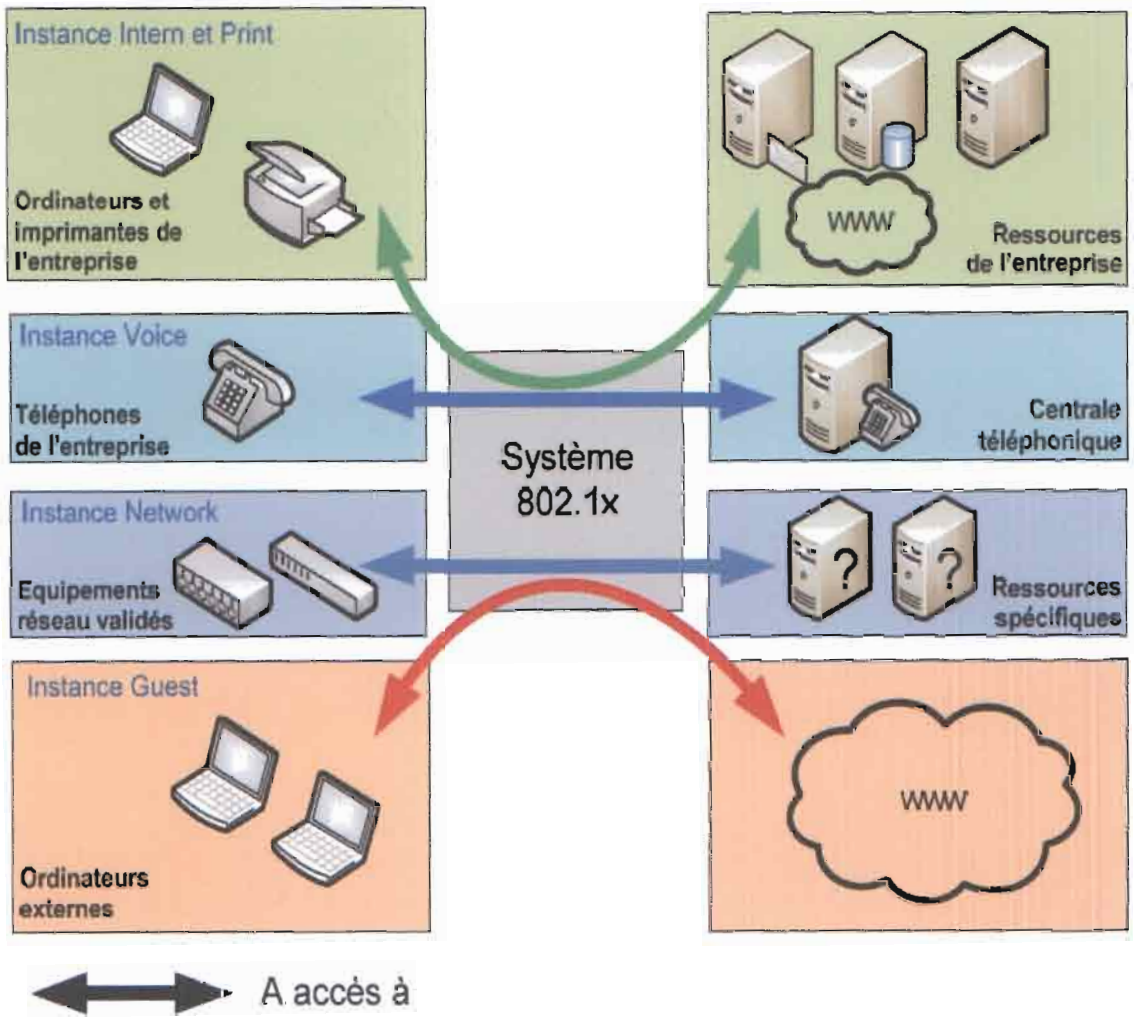


Figure 9 : Illustration des droits d'accès

3.2.4 Types d'interfaces

Les différentes instances de connexion au réseau nécessitent des types de ports différents dans leur principe de configuration. Voici donc le tableau récapitulatif des différents types de ports selon les instances :

Tableau 7 : les interfaces de connexion

	Desktop Port	Printer Port	Multi-Port
Instance	Intern + Voice	Print	**Intern + Guest**
Type de hosts	Multi Domain Acces	Single Host	n/a
Attribution VLAN	Automatique	Automatique	Trunk
Type d'authentification	EAP-TLS + Physique Adress Bypass	Physique Adress Bypass	n/a
Restrictions Un équipement par	Domain (1 data + 1 voice)	Un équipement par port	n/a
Remarques	Ports dédiés pour les bureaux et salles de conférences Un seul port pour téléphone + ordinateur	Ports dédiés pour imprimantes uniquement	Port dédié pour cascader des Switch. Il s'agit d'une liaison Trunk entre le Switch 802.1 et des Switch d'extensions compatible 802.1x

Le serveur RADIUS NPS a pour mission de centraliser l'authentification et l'autorisation en s'appuyant généralement sur Active Directory.

3.3.1 Conception des méthodes et les stratégies de connexion

Nous définissions les stratégies de connexion NPS (Policy) suivantes :

- **Connection request Policy :** pour savoir si la requête reçue sera traitée par ce serveur RADIUS ou non. Cette Policy traitera toutes les demandes de connexion de type « filaire » via le commutateur.
- **Policy IP-Phones :** pour l'authentification des téléphones IP grâce à leurs adresses physique

- **Policy Printers :** pour l'authentification des imprimantes de l'entreprise grâce à leurs adresses physiques.

- **Policy Network :** pour l'authentification des imprimantes de l'entreprise grâce à leurs adresses PHYSIQUES.

- **Policy Intern :** pour l'authentification des ordinateurs de la société grâce à leur nom d'ordinateur et leur certificat machine. Cette Policy représente l'ensemble des Policies des groupes machine des différentes directions, dans la pratique.

3.3.2 Conception des méthodes de contrôle d'accès

Après l'authentification du client, le RADIUS retourne au NAS un certain nombre d'attributs-valeurs pour permettre le basculement du client réseau dans le VLAN prédéfini. Pour affecter un client sur un VLAN prédéfini les attributs suivants doivent être transmis depuis le RADIUS vers le NAS avec les valeurs suivantes :

Tunnel-mediumType

Tunnel-Type

Tunnel-Private-Group-Id

En fonction des instances et des groupes de machine, nous définissons ces attributs. De façon générale **Tunnel-mediumType: IEEE-802 et Tunnel-Type: VLAN.** Suivant chaque instance et groupe d'ordinateurs, nous avons Tunnel-Private-Group-Id: **"ID du VLAN de l'instance ou du groupe d'ordinateur".**

Avec ces valeurs, le NAS basculera le port de connexion du client sur le VLAN prédéfini. Des attributs propriétaires (Vendors Specific Attributs) permettent d'adapter la configuration du NAS en fonction des autorisations à accorder au client. Sur les matériels HP, l'attribut HP-IP-FILTER-RAW permet de mettre en place une règle de filtrage (ACE1) qui sera appliquée au trafic entrant du client sur le port du NAS. Ainsi, les attributs-valeurs permettent d'adapter la connexion du client réseau, indépendamment de ce dernier, aux ressources auxquelles il peut prétendre : Un

téléphone IP aura besoin du VLAN de la ToIP et de trafic prioritaire, un client ordinaire sera redirigé dans le VLAN de son groupe habituel sans restriction.

3.4.1 Description

Le fonctionnement du système de contrôle d'accès dans son ensemble suit le principe de la défense en profondeur (en annexe V). Suivant le niveau d'avancement de l'utilisateur, de nouveau contrôle lui sont soumis. La figure 10 ci-après présente les différents niveaux de contrôle et les contrôles effectués.

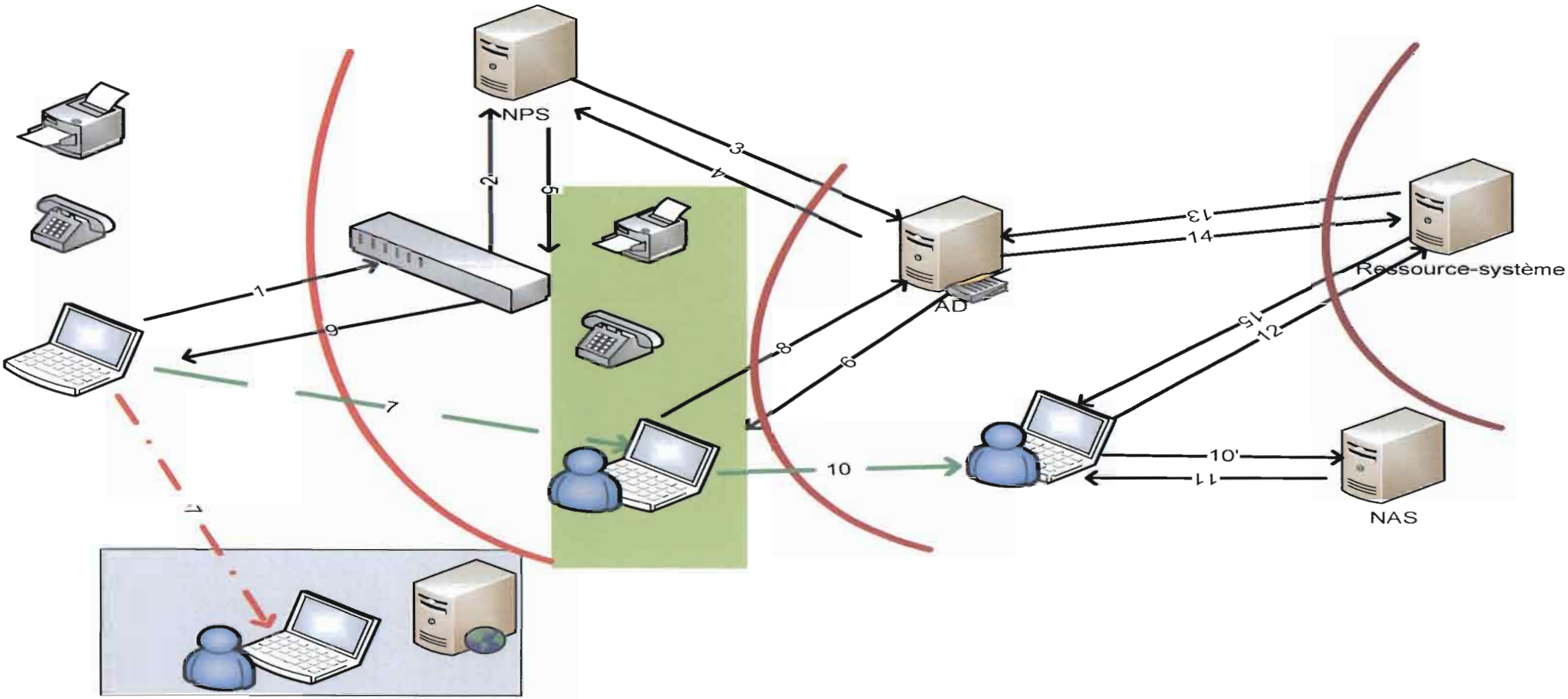


Figure 10 : Architecture fonctionnelle

1. Le poste de travail se branche sur un des ports du commutateur. Le suppliant va envoyer vers le serveur RADIUS les éléments d'authentification (certificat, identifiant, mot de passe...).

2. Le commutateur détecte cette connexion et envoie une requête d'authentification

(Access-Request) au serveur RADIUS.

3. le serveur RADIUS interroge l'annuaire avec, l'identifiant donnée par le suppliant.

4. l'annuaire confirme ou infirme, l'identité.

5. le serveur accepte ou refuse l'authentification et renvoie sa réponse au commutateur

6. Commutateur ouvre le port sur le VLAN commandé par le serveur.

7. la machine (l'équipement réseau) est placé dans un VLAN spécifique. Pour la machine du service il est placé dans le VLAN du service. L'utilisateur peut ainsi avoir accès au domaine.

8. Pour accéder au domaine l'utilisateur saisit son login et son mot de passe. La machine envoie une requête d'authentification au contrôleur de domaine.

9. le contrôleur de domaine identifie l'utilisateur en commandant l'ouverture ou le mot de la session.

10, 10' et 11. Lors de l'ouverture de la session la machine charge le profile utilisateur sous le contrôle du contrôleur de domaine.

12. A la demande de l'utilisateur d'accéder à un fichier.

13. Le serveur de fichier vérifie auprès de l'annuaire le groupe d'utilisateur de l'utilisateur et

14. au sein de son ACL les autorisations (permission) de son groupe sur les fichiers,

15. pour l'appliquer

3.4.2 Exigence fonctionnelle

L'exigence de disponibilité de l'annuaire AD et du serveur NPS est par principe très élevée. Car généralement, ils interviennent directement lors des contrôles d'accès qu'assurent les mécanismes de contrôle d'accès. L'annuaire AD intervient d'une manière coopérative sur les annuaires de sécurité (exemple : ACL) des mécanismes de contrôle d'accès. Cependant, ces derniers doivent être très performants et hautement disponibles pour assurer la qualité du service du Système d'information global.

L'interruption du fonctionnement du « provisioning » n'a pas d'impact fort sur le fonctionnement d'ensemble du système de contrôle d'accès. Quelques fonctions peuvent éventuellement imposer des contraintes plus fortes. Notamment, les fonctions de self-service de changement du mot de passe et de déblocage des comptes dans le cas des oublis (des mots de passe). Mais là encore, le risque encouru est limité à l'impossibilité d'accéder au système d'information d'un ou de quelques utilisateurs.

Notre réseau est soumis à des contraintes de performance toujours plus élevées. Dans ce contexte, les incidents peuvent être lourds de conséquences en termes de fonctionnement. Aussi, est-il indispensable de superviser le trafic réseau afin de maintenir une qualité de service optimale. Cette supervision, sur un réseau commuté, doit être effectuée sur chaque point d'accès, afin de disposer d'éléments précis sur le trafic de chaque client connecté. Dès lors, il devient possible de mettre en évidence les anomalies de fonctionnement et/ou les comportements suspects des clients et de planifier des actions automatiques (ou semi-automatiques) en réponse.

Pour établir la validation du concept, nous allons créer un laboratoire d'un réseau prototype (dans un environnement virtuel) qui va nous permettre de valider notre solution avec les objectifs et les contraintes du cahier des charges. Ce

laboratoire sera légèrement simplifié par rapport au réseau actuel dans l'entreprise mais comportera tous les composants principaux nécessaires à la validation du concept.

4.1.1 Moyens nécessaires

Voici un tableau 7 récapitulant les acteurs principaux obligatoires et facultatifs pour valider le concept :

Tableau 8 : les éléments nécessaires

Objet	Acteur	Rôle	Utilisation
Switch Multicouches	Réseau	Authentificateur 802.1x Simulation de l'infrastructure réseau de la société	Obligatoire
Serveur Windows	Système	Simulation du contrôleur de domaine	Obligatoire
Serveur Web		Simulation d'internet	Obligatoire
Serveur NAS	Système	Stockage réseau de la société	Obligatoire
2 Ordinateurs	Client	Simulation ordinateur de la société et Guest	Obligatoire
Téléphone IP	Client	Simulation authentification téléphone IP	Obligatoire
Imprimante	Client	Réseau Simulation authentification imprimante de la société	Obligatoire
Mini-Switch de bureau	Réseau /Client	Simulation de connexion d'un Switch nomade + extension de ports	Obligatoire
Hub	Réseau /Client	Simulation de contournement de 802.1x	Facultatif

4.1.2 Schéma réseau physique

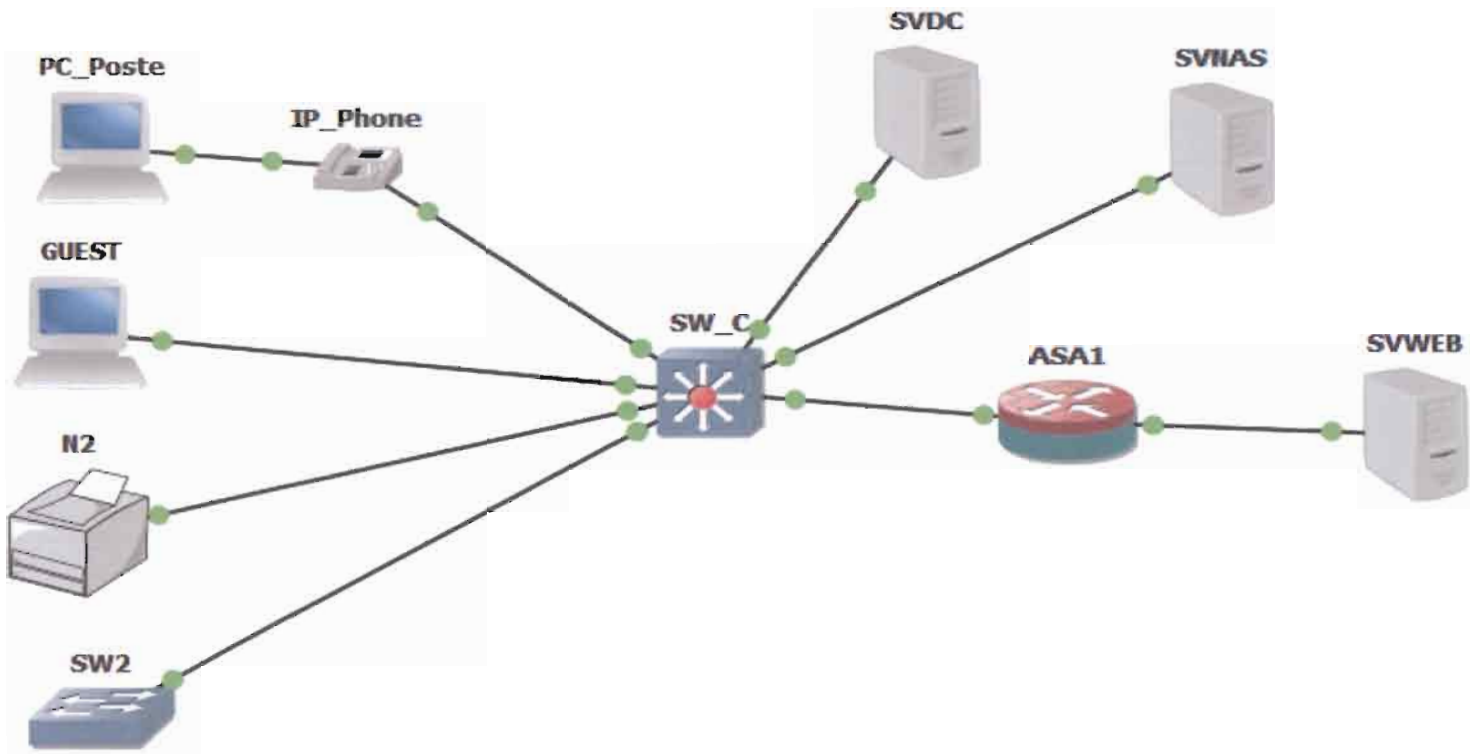


Tableau 9 : Schéma physique du prototype

4.2.1 Le Switch central 802.1x (SW-C-000)

1. Option de base

Commande	Description
`hostname SW-C-000`	Définition du nom du Switch
`ip name-server 10.0.100.100`	Définition du serveur DNS
`spanning-tree portfast bpduguard default`	Activation du bpduguard sur toutes les interfaces spanning-tree portfast

2. 802.1x base

Commande	Description
`aaa new-model`	Activation de AAA (Authorization, Authentication, Administration)
`aaa authentication dot1x default group RADIUS`	Crée une liste de méthode d'authentification 802.1x en ajoutant la méthode RADIUS
`dot1x system-auth-control`	Activation du 802.1x de façon générale
`aaa authorization network default group RADIUS`	Permet une assignation dynamique des VLAN par RADIUS
`dot1x guest-VLAN supplicant`	Autorise également les supplicants compatibles 802.1x d'être affectés au VLAN Guest en cas d'échec d'authentification
`RADIUS-server host 10.0.100.100 auth-port 1645 acct-port 1646` `RADIUS-server key 12345678`	Définition du serveur RADIUS ainsi que la clef de cryptage pour la communication

3. Ports

FastEthernet 0/1 à 0/6 :

Commande	Description
`switchport mode access`	Définition du type access du port
`switchport voice VLAN 5`	Définition statique du VLAN voix
`authentication event fail action authorize VLAN 3`	Si le supplicant échoue à l'authentification il sera placé dans le VLAN 3 (Guest)

`authentication event no-response action authorize VLAN 3`	Si le supplicant ne répond pas aux demandes d'authentification il sera placé dans le VLAN 3 (Guest)
`authentication host-mode multi-domain`	Définition de l'authentification multi domaine
`authentication order mab dot1x`	Commencer d'abord par MAB et si cela échoue passer à 802.1x
`authentication priority mab dot1x`	Donner la priorité à MAB puis si cela échoue passer à 802.1x
`authentication port-control auto`	Activation de l'authentification 802.1x
`authentication periodic`	Activation de l'authentification périodique (chaque heure) des supplicants déjà autorisés
`authentication violation protect`	Lors d'une violation de sécurité, le port passe en mode protected et empêche le trafic pour les nouvelles adresses physique
`mab`	Activation du Physique Adress Bypass
`dot1x pae authenticator`	Activation du mode authentificateur
`authentication periodic`	Activation de la réauthentification périodique
`dot1x timeout quiet-period 10`	Temps d'attente en secondes avant de renvoyer une demande d'authentification quand celle-ci a échoué (max. 2 tentatives)
`dot1x timeout tx-period 5`	Temps d'attente en secondes d'une réponse du supplicant
`spanning-tree portfast`	Passage direct de l'état « blocking » à l'état forwarding.
`authentication event server dead action authorize VLAN 3`	Permettre le passage dans le VLAN Guest si le serveur RADIUS ne répond pas.
`authentication event server alive action reinitialize`	Réinitialiser les connexions déjà authentifiées lorsque le serveur RADIUS revient en ligne.

FastEthernet 0/7 à 0/8 :

Commande	Description
`switchport mode access`	Définition du type access du port
`authentication event fail action authorize VLAN 3`	Si le supplicant échoue à l'authentification il sera placé dans le VLAN 3 (Guest)
`authentication event no-response`	Si le supplicant ne répond pas aux

`action authorize VLAN 3`	demandes d'authentification, il sera placé dans le VLAN 3 (Guest)
`authentication host-mode single-host`	Définition de l'authentification single-host
`authentication order mab dot1x`	Commencer d'abord par MAB et si cela échoue passer à 802.1x
`authentication priority mab dot1x`	Donner la priorité à MAB puis si cela échoue passer à 802.1x
`authentication port-control auto`	Activation de l'authentification 802.1x
`authentication periodic`	Activation de l'authentification périodique (chaque heure) des supplicants déjà autorisés
`authentication violation protect`	Lors d'une violation de sécurité, le port passe en mode protected et empêche le trafic pour les nouvelles adresses physique.
`mab`	Activation du Physique Adress Bypass
`dot1x pae authenticator`	Activation du mode authentificateur
`authentication periodic`	Activation de la réauthentification périodique
`dot1x timeout quiet-period 10`	Temps d'attente en secondes avant de renvoyer une demande d'authentification quand celle-ci a échoué (max. 2)
`dot1x timeout tx-period 5`	Temps d'attente en secondes d'une réponse du supplicant
`spanning-tree portfast`	Passage direct de l'état « blocking » à l'état forwarding.
`authentication event server dead action authorize VLAN 3`	Permettre le passage dans le VLAN Guest si le serveur RADIUS ne répond pas.
`authentication event server alive action reinitialize`	Réinitialiser les connexions déjà authentifiées lorsque le serveur RADIUS revient en ligne.

FastEthernet 0/9 à 0/11 :

Commande	Description
`switchport port trunk encapsulation dot1q`	Définition tu type d'encapsulation dot1q
`switchport trunk native VLAN 100`	Définition du VLAN native 100. A la réception d'une trame non « tagguée » celle-ci sera assignée dans le VLAN 100
`switchport allowed VLAN 2,3,100`	Seuls les VLAN 2,3,100 sont autorisés sur

	ce port
`switchport mode trunk`	Définition du type de port en trunk
`switchport no negotiate`	Désactivation de la négociation

FastEthernet 0/12 à 0/13:

Commande	Description
`switchport mode access`	Définition du type access du port

FastEthernet 0/14 :

Commande	Description
`switchport trunk encapsulation dot1q`	Définition du type de trunk
`switchport trunk allowed VLAN 2,3,5,10,100`	Définition des VLANs autorisés
`switchport mode trunk`	Définition de type de port trunk

FastEthernet 0/15 :

Commande	Description
`switchport mode access`	Définition du type access du port
`switchport access VLAN 100`	Accès du port au VLAN 100

4.2.2 Le contrôleur de domaine (SVDC)

1. Active Directory

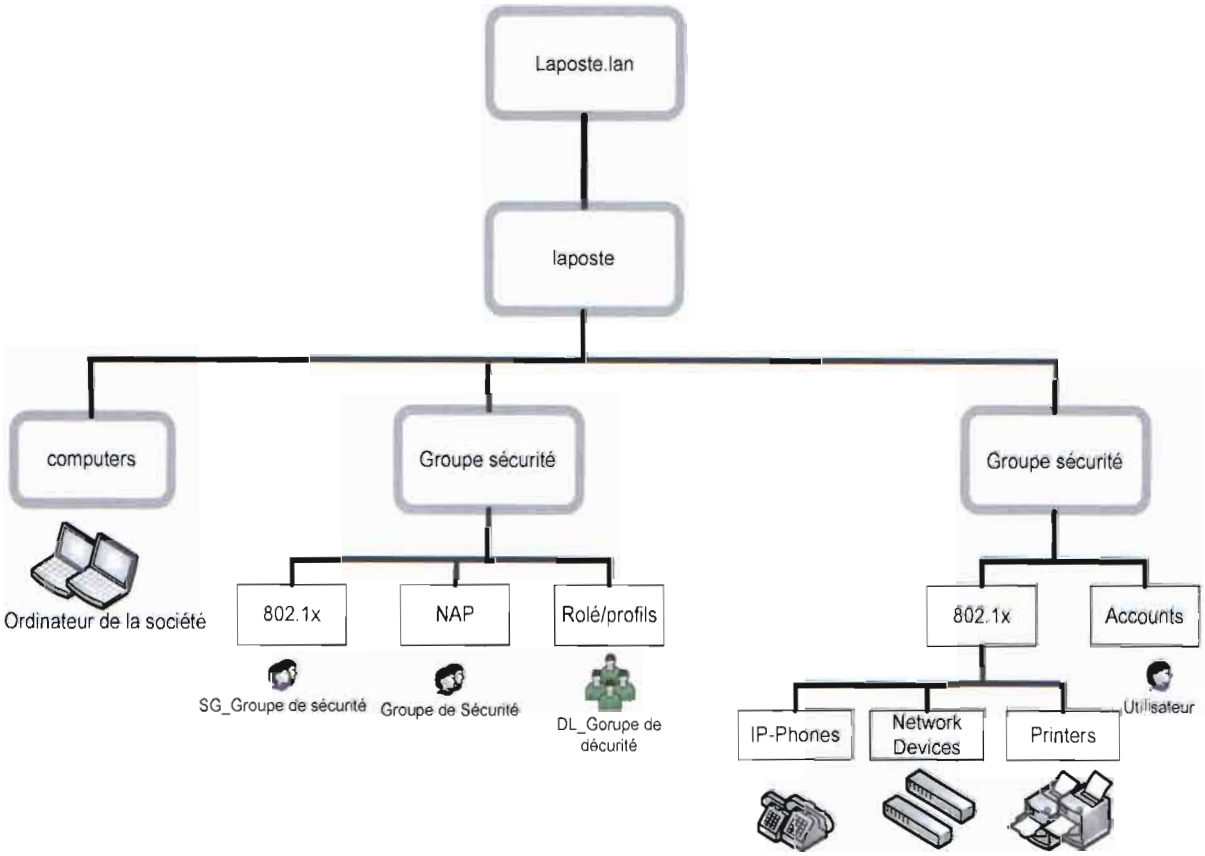
L'active Directory est la base de données des utilisateurs et des équipements réseau de notre domaine laposte.lan. C'est sur cette base de données que le service NPS va s'appuyer pour identifier les supplicants qui sont autorisés à accéder au réseau d'entreprise.

Installation

Installation standard d'Active Directory et du domaine laposte.lan avec la commande dcpromo.exe.

Configuration

Création d'une arborescence LDAP simple :



Les unités organisationnelles ont été créées pour organiser les différents éléments LDAP à savoir : utilisateurs AD, utilisateurs 802.1x, machines et groupes de sécurité, pour maintenir un certain ordre au sein d'Active Directory.

Les utilisateurs

Au sein de notre Active Directory, nous avons deux types d'utilisateurs :

- **Utilisateur « Accounts » :**

Ces utilisateurs sont destinés à la connexion au domaine sur les ordinateurs professionnels de la société.

- **Utilisateurs 802.1x**

Ce sont des utilisateurs spéciaux pour l'authentification MAB. En effet, ils portent comme « username » et comme mot de passe l'adresse physique du supplicant à accepter au réseau.

La définition de l'adresse physique comme mot de passe peut faire conflit avec la politique de complexité des mots de passe de la société. Pour notre prototype, il a été nécessaire de désactiver la politique de mot de passe standard d'Active Directory pour faire accepter l'adresse physique.

Les compte d'ordinateur :

Nous avons des comptes d'ordinateurs standard et des unités des ordinateurs par direction et les services.

Groupes de sécurité

- **802.1x et NAP**

Pour que notre NPS puisse authentifier nos différents supplicants, il faut lui fournir un groupe de sécurité dans lequel il va contrôler l'identité du supplicant, nous avons donc créé les groupes suivants :

Nom	Type
SG_GL_802.1x-computers	Groupe de sécurité - Global
SG_GL_802.1x-IP-Phone	Groupe de sécurité - Global
SG_GL_802.1x-Nework-Divices	Groupe de sécurité - Global
SG_GL_802.1x-Printers	Groupe de sécurité - Global

✓ **SG_GL_802.1x-Computers :**

Groupe contenant les comptes machines des ordinateurs d'entreprise.

✓ **SG_GL_802.1x-IP-Phones :**

Groupe contenant les users d'adresses physique des différents téléphones IP de la société.

✓ **SG_GL_802.1x-Network-Devices :**

Groupe contenant les users d'adresses physique des différents Switch 802.1x validés par la société.

✓ **SG_GL_802.1x-Printers :**

Groupe contenant les users d'adresses physique des différentes imprimantes de la société.

- **Les Groupe utilisateur**

Pour que les serveurs puissent autoriser l'accès des utilisateurs aux fichiers, il faut leurs fournir un groupe de sécurité dans lequel ils vont contrôler l'identité de l'utilisateur, nous avons donc créé les groupes suivants :

✓ **SG_GL_Direction :**

Groupe contenant les utilisateurs de la direction.

✓ **SG_GL_Division1:**

Groupe contenant les utilisateurs de la division1.

✓ **SG_GL_Division2:**

Groupe contenant les utilisateurs de la division2.

✓ **SG_GL_Section1 :**

Groupe contenant les utilisateurs de la section1.

✓ **SG_GL_Section2 :**

Groupe contenant les utilisateurs de la section2.

✓ **DL_SV_Directiondoc_nodif :**

Groupe contenant les utilisateurs ou groupe d'utilisateurs ayant droit de notification (lecture, écriture, exécution) sur la ressource « Directiondoc »

✓ **DL_SV_Directiondoc_lecture :**

Groupe contenant les utilisateurs ou groupe d'utilisateurs ayant droit de lecture sur la ressource « Directiondoc »

✓ **DL_SV_Directiondoc_deny :**

Groupe contenant les utilisateurs ou groupe d'utilisateurs n'ayant aucun droit sur la ressource « Directiondoc »

- ✓ **DL_SV_Division1doc_nodif :**

Groupe contenant les utilisateurs ou groupe d'utilisateurs ayant droit de notification (lecture, écriture, exécution) sur la ressource « Division1doc »

- ✓ **DL_SV_Division1doc_lecture:**

Groupe contenant les utilisateurs ou groupe d'utilisateurs ayant droit de lecture sur la ressource « Division1doc »

- ✓ **DL_SV_Division1doc_deny**:

Groupe contenant les utilisateurs ou groupe d'utilisateurs n'ayant aucun droit sur la ressource « Division1doc »

- ✓ **DL_SV_Division2doc_nodif :**

Groupe contenant les utilisateurs ou groupe d'utilisateurs ayant droit de notification (lecture, écriture, exécution) sur la ressource « Division2doc »

- ✓ **DL_SV_Division2doc_lecture:**

Groupe contenant les utilisateurs ou groupe d'utilisateurs ayant droit de lecture sur la ressource « Division2doc »

- ✓ **DL_SV_Division2doc_deny:**

Groupe contenant les utilisateurs ou groupe d'utilisateurs n'ayant aucun droit sur la ressource « Division2doc »

- ✓ **DL_SV_Section1doc_nodif :**

Groupe contenant les utilisateurs ou groupe d'utilisateurs ayant droit de notification (lecture, écriture, exécution) sur la ressource « Section1doc »

- ✓ **DL_SV_Section1doc_lecture:**

Groupe contenant les utilisateurs ou groupe d'utilisateurs ayant droit de lecture sur la ressource « Section1doc »

- ✓ **DL_SV_Section1doc_deny:**

Groupe contenant les utilisateurs ou groupe d'utilisateurs n'ayant aucun droit sur la ressource « Section1doc »

- ✓ **DL_SV_Section2doc_nodif :**

Groupe contenant les utilisateurs ou groupe d'utilisateurs ayant droit de notification (lecture, écriture, exécution) sur la ressource « Section2doc»

- ✓ **DL_SV_Section2doc_lecture:**

Groupe contenant les utilisateurs ou groupe d'utilisateurs ayant droit de lecture sur la ressource « Section2doc »

- ✓ **DL_SV_Section2doc_deny :**

Groupe contenant les utilisateurs ou groupe d'utilisateurs n'ayant aucun droit sur la ressource « Section2doc»

- **Le GPO**

- ✓ **GPO_ordi_profils_itinérants :**

GPO de création des Profils itinérants des utilisateurs sur le serveur.

- ✓ **GPO_user_mappage Data :**

Mettre en place un lecteur réseau sur le répertoire **DSI**

- ✓ **GPO_user_deploiement WIN:**

Installation du logiciel **chrome et office**

- ✓ **GPO_user_options-dossiers :**

GPO permettant de ne pas masquer les extensions des fichiers et de ne pas sélectionner le partage de fichier

2. DNS

Le service DNS se charge de la résolution de nom de domaines tels que des noms de machines et des serveurs. Pour notre prototype, ce service simule aussi l'internet et plus précisément la zone google.bf

Installation

Le service DNS est installé par défaut lors de l'installation de l'Active Directory avec la commande dcpromo.exe

Configuration

- **Forward Lookup Zones**

Configuration standard avec une zone de résolution de conversion de nom en adresses IP : **laposte.lan ;**

Création d'une zone spéciale google.ch avec un hôte www portant l'adresse IP 10.0.200.100 qui correspond au serveur web

- **Reverse Lookup Zones**

Configuration standard avec une zone de résolution inversée par VLAN

3. DHCP

Le service DHCP distribue les adresses IP correspondant aux différents VLAN et leurs sous-réseaux.

Installation

Installation standard du rôle DHCP par le biais du server manager.

Configuration

- **Scopes**

Configuration de 3 scopes d'adresses pour les VLANs clients suivants :

VLAN 2 – Intern

VLAN 3 – Guest

VLAN 5 – Voice

- **Options**

Pour chaque scope, les options suivantes ont été configurées :

- **003 Router :** indique la passerelle par défaut pour chaque VLAN
- **006 DNS Servers :** indique le serveur DNS du domaine
- **015 DNS Domain Name :** Indique le nom du domaine

- **Options spécifiques**

Pour les téléphones IP CISCO, une option DHCP spéciale est nécessaire pour qu'ils acceptent le « lease ».

L'Option spéciale **150 CISCO IP-Phone**

TFTP Server définit le serveur TFTP **10.0.100.100** sur lequel ils vont télécharger leur configuration.

Dans notre cas, aucun service TFTP n'est activé sur le serveur 10.0.100.100, mais l'option est nécessaire pour le téléphone.

4. L'autorité de certification

L'autorité de certification gère, émet et révoque les différents certificats numériques du domaine laposte.lan. Pour notre prototype, ce rôle permet l'établissement de certificats machines pour les ordinateurs de la société afin de les authentifier via la méthode EAP-TLS.

Pour cette méthode d'authentification, un certificat côté supplicant n'est pas obligatoire, mais son utilisation nous permet de pouvoir révoquer ces certificats en cas de vol de machine par exemple. C'est pour cela que nous avons choisi d'utiliser un certificat côté serveur et côté supplicant.

Installation

Installation standard du rôle « Active Directory Certificate Services » par le biais du « Server Manager ». Dans ce rôle nous avons uniquement choisi la fonction « Certification Authority ».

Son installation va en outre créer automatiquement un certificat « Root CA » racine pour le domaine contrôleur. Ce certificat est quant à lui obligatoire pour une authentification EAP-TLS puisque le contrôleur de domaine et/ou le serveur RADIUS (dans notre cas, le même serveur) doivent s'identifier envers le supplicant qui doit porter ce certificat dans son gabarit des autorités de certification autorisées

Configuration

Aucune configuration spécifique n'a été faite pour ce service.

5. Le service Network Policy Server (NPS)

Le service NPS est un acteur important dans l'authentification 802.1x car c'est l'élément qui authentifie les différents supplicants auprès de la base de données Active Directory. C'est au sein de ce service qu'on configure nos règles d'accès sous forme de « Policy ».

Installation

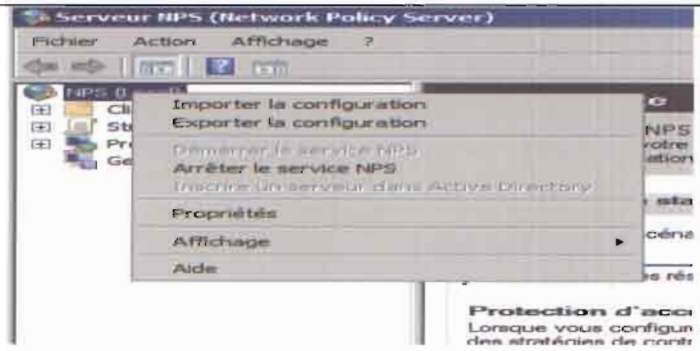
Installation standard du rôle « Network Policy and Access Services », ce fait par le biais du « Server Manager ».

Dans ce rôle nous avons uniquement choisi la fonction « Network Policy Server ».

Configuration

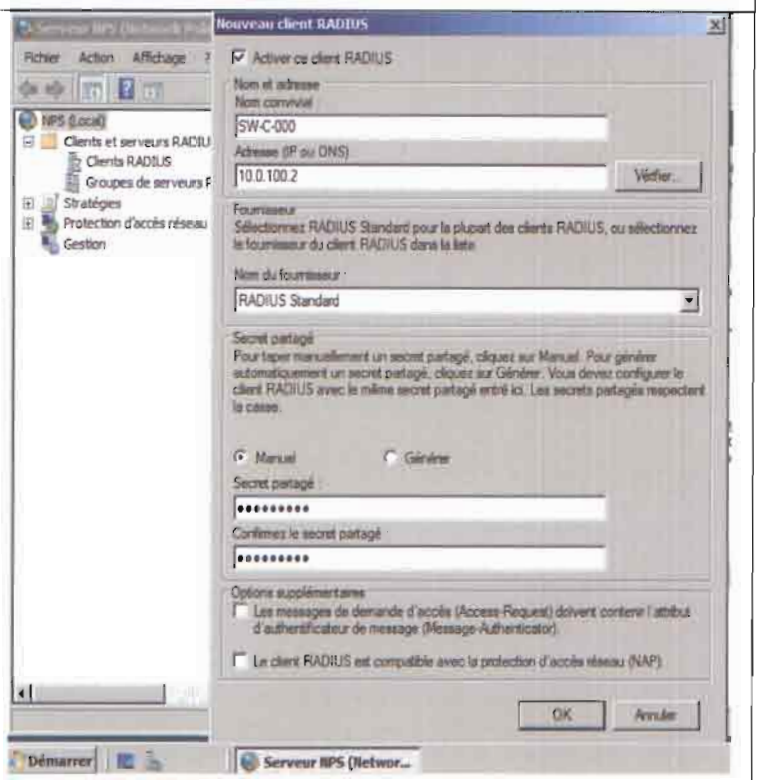
- **Enregistrement dans Active Directory**

Pour que le service NPS soit autorisé à faire des requêtes LDAP dans Active Directory, il faut l'enregistrer.

Ouvrir la console de gestion NPS sous **Administrative Tools** ➡ **Network Policy Server**	
Clic droit sur : **NPS (Local)** puis choisir : **Register service in Active Directory** Valider la boite de dialogue suivante	

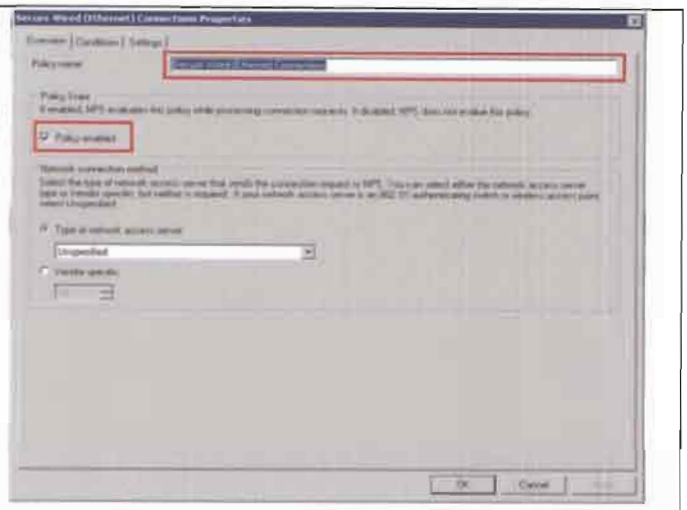
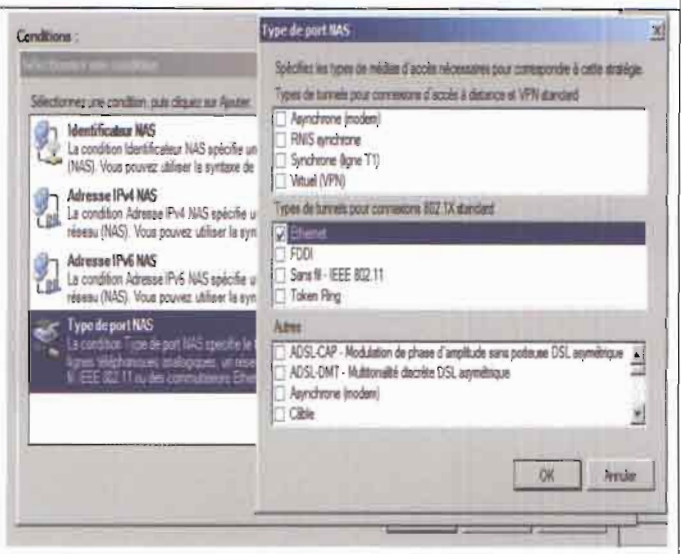
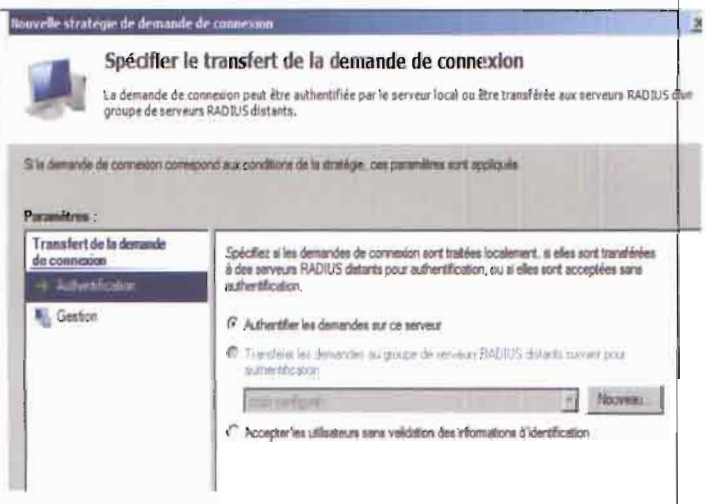
- **Ajout d'un client RADIUS**

Avant de pouvoir recevoir des requêtes RADIUS, il faut ajouter un client RADIUS autorisé à contacter ce serveur NPS

Dans la console de gestion. Développer **RADIUS Clients and Servers** Faire un clic droit sur **RADIUS Clients** Choisir **New**	
Sous **Friendly name** Saisir le nom du client RADIUS Saisir l'adresse IP Choisir une clé secrète **Shared secret** à configurer aussi sur le client RADIUS Valider par OK	

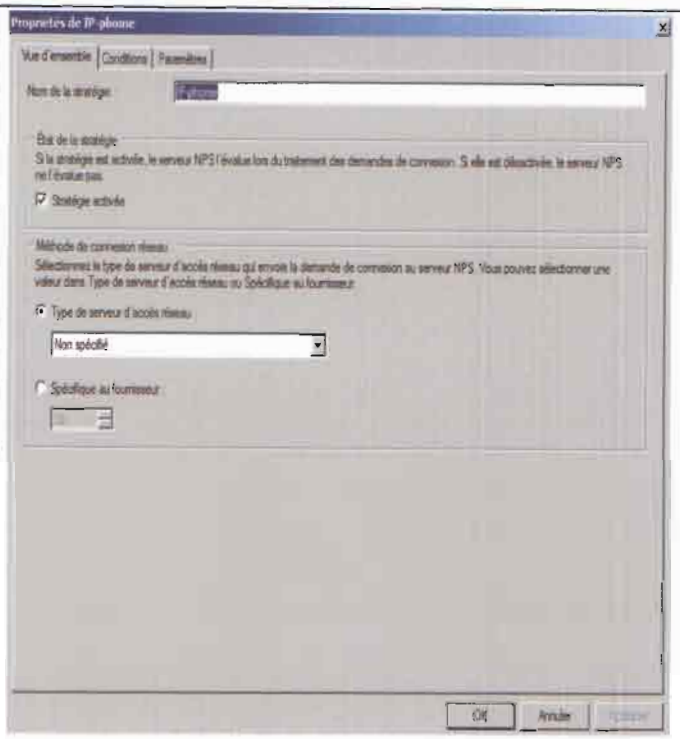
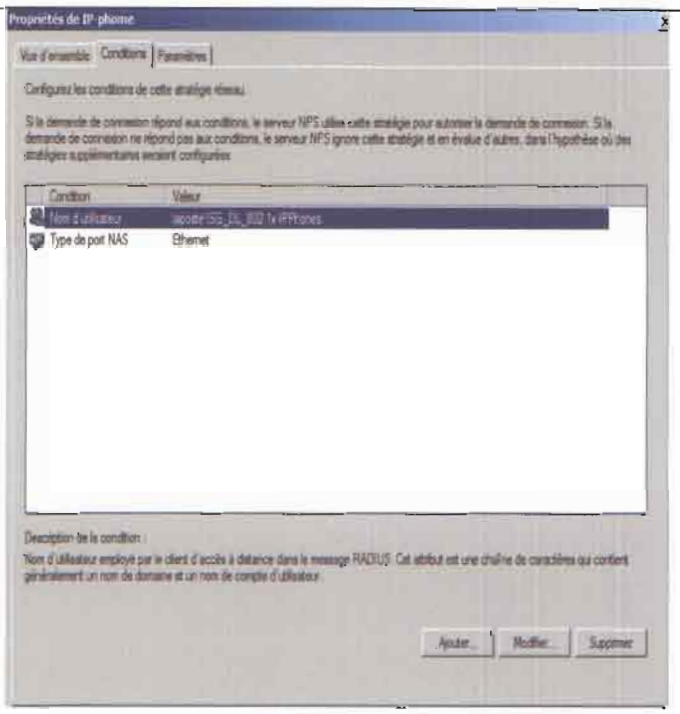
1. **Connection request Policy**

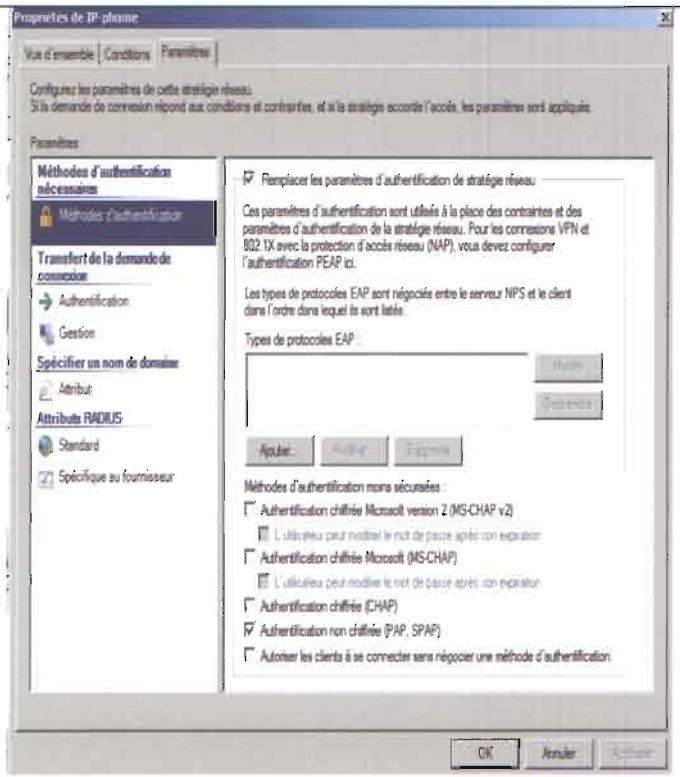
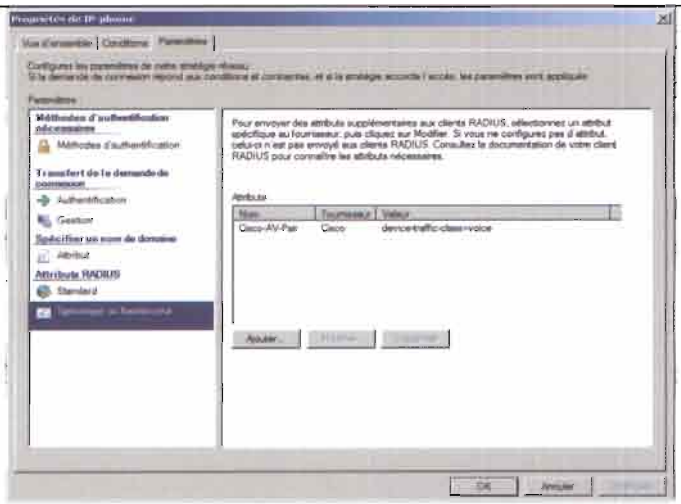
Cette Policy détermine si la requête reçue sera traitée par ce serveur RADIUS ou non. Pour notre prototype, nous avons créé une Policy qui traite toutes les demandes de connexion de type « filaire »

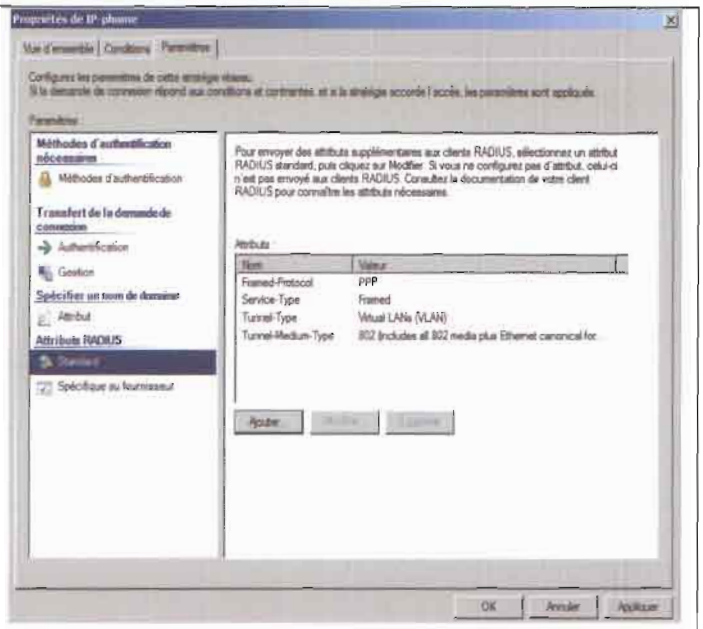
Saisir le nom de la Policy sous Policy name Activer la Policy en cochant Policy Enabled	
Sous l'onglet **Conditions** Cliquer sur bouton **Add** pour ajouter condition Choisir catégorie **NAS Port Type** Sous **Common 802.1X connexion tunnel types** Choisir **Ethernet** Valider par OK	
Sous l'onglet **Settings** Choisir catégorie **Authentication** Choisir **Authenticate requests on this server** Valider par OK	

2. Policy IP-Phones

Cette Policy authentifie les téléphones IP grâce à leurs adresses physique

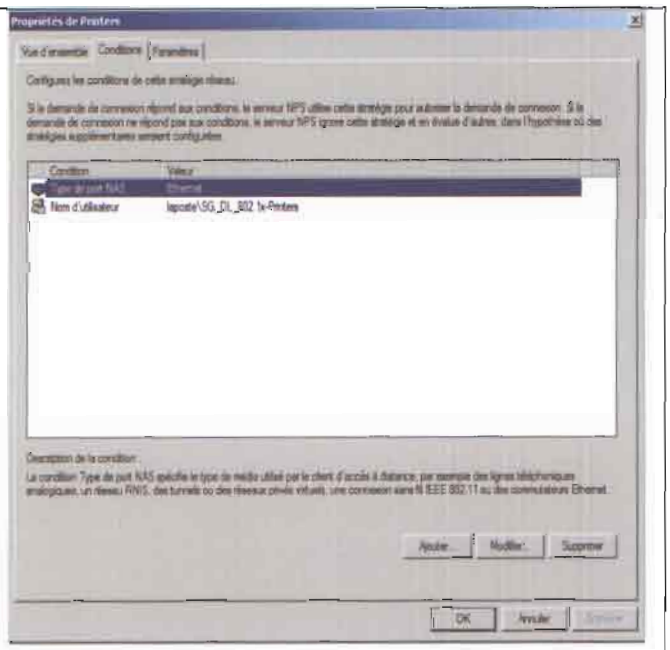
Saisir le nom de la Policy sous **Policy name** Activer la Policy en cochant **Policy Enabled** Choisir **Grant access. Grant access** **if the connection** **request matches this** **policy** Cocher **Ignore user account dailin properties**	
Sous l'onglet **Conditions** Ajouter la condition **NAS Port Type Ethernet** Et la condition **User Groups** **laposte\SG-DL-802.1x-IPPhones** qui correspond au groupe de sécurité contenant les users avec les adresses physique des téléphones IP	

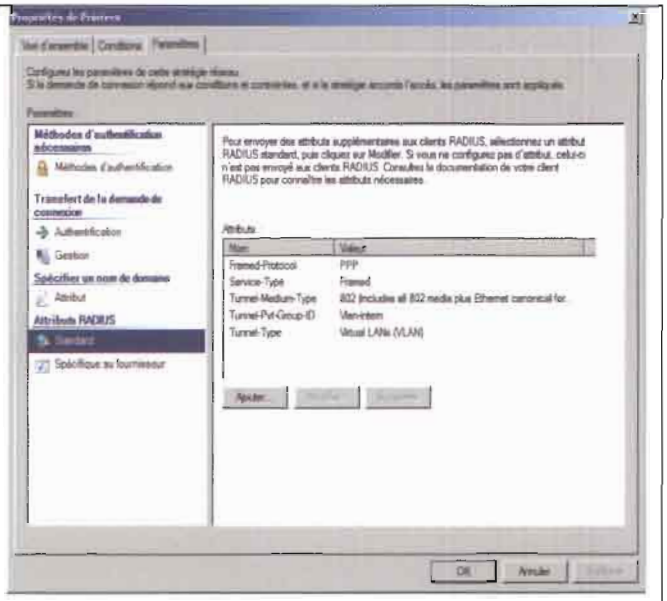
Sous l'onglet **Contraints** Choisir la catégorie **Authenticaton Methods** Supprimer tous les types EAP dans la liste et cocher uniquement **Unencrypted authentication** cette méthode correspond à l'envoi en « clair » de l'adresse physique du supplicant par le Switch	
Sous l'onglet **Settings et la catégorie Standard** Ajouter les attributs suivants: **Framed-Protocol** : PPP **Service-Type :** Framed **Tunnel-Medium-Type** :802 **Tunnel-Type :** Virtual Lans	

Sous la catégorie **Vendor Specific** Ajouter l'attribut **Cisco-AV-Pair** avec comme valeur **device-traffic-class=voice** qui indique l'utilisation du domaine voice sur des ports MDA Confirmer par OK	

- **Policy Printers**

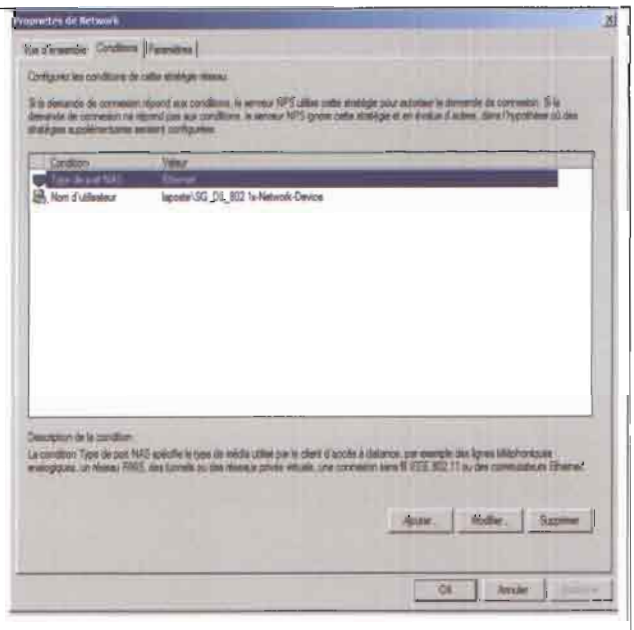
Cette Policy authentifie les imprimantes de l'entreprise grâce à leurs adresses PHYSIQUE. Les paramètres de cette policy sont identiques à la Policy IP-Phones sauf les paramètres suivants

Sous l'onglet Conditions Ajouter la condition **NAS Port Type Ethernet** et la condition qui correspond au groupe de sécurité contenant les users avec les adresses physique des imprimantes User Groups **laposte\SG-DL-802.1x-Printers**	

Sous l'onglet **Settings** et la catégorie Standard Ajouter les attributs suivants: **Framed-Protocol** : PPP **Service-Type** : Framed **Tunnel-Medium-Type** : 802 **Tunnel-Type** : Virtual Lans **Tunnel-Pvt-GroupID** : VLAN-intern Cette valeur correspond à l'assignation de VLAN et dans ce cas du VLAN-intern (VLAN 2)	
L'attribut sous la catégorie **Vendor Specific** utilisé pour la Policy voice est à retirer	

- **Policy Network**

Cette Policy authentifie les imprimantes de l'entreprise grâce à leurs adresses PHYSIQUE. Les paramètres de cette Policy sont identiques à la Policy IP-Phones sauf les paramètres suivants :

Sous l'onglet **Conditions** Ajouter la condition **NAS Port Type Ethernet** Et la condition **User Groups** **laposte\SG-DL-802.1x-Network-Devices** qui correspond au groupe de sécurité contenant les users avec les adresses physique des Switch 802.1x validés	

Sous l'onglet **Settings** et la catégorie **Standard**

Ajouter les attributs suivants :

Framed-Protocol : PPP

Service-Type : Framed

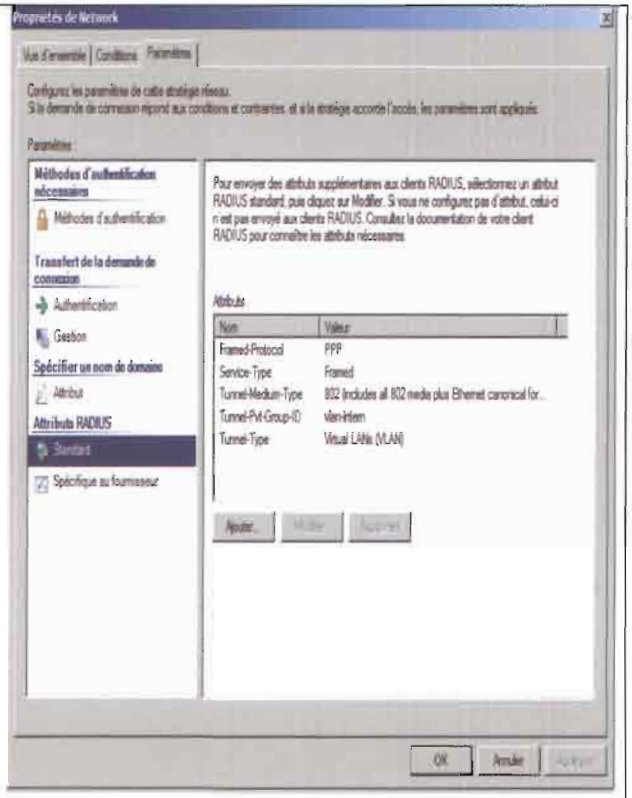
Tunnel-Medium-Type : 802

Tunnel-Type : Virtual Lans

Tunnel-Pvt-GroupID : VLAN-intern

Cette valeur correspond à l'assignation de VLAN.

Pour illustrer l'exemple, nous avons affecté le VLAN 2 (VLAN-intern) pour simuler l'ajout d'un Switch d'extension qui aura son interface management dans le réseau 10.0.2.0/24



L'attribut sous la catégorie **Endor Specific**

utilisé pour la Policy Voice est à retirer

- **Policy Intern**

Cette Policy authentifie les ordinateurs de l'entreprise grâce à leur nom d'ordinateur et leur certificat machine. Les paramètres de cette Policy sont identiques à la Policy IP-Phones sauf les paramètres suivants :

Sous l'onglet **Conditions**

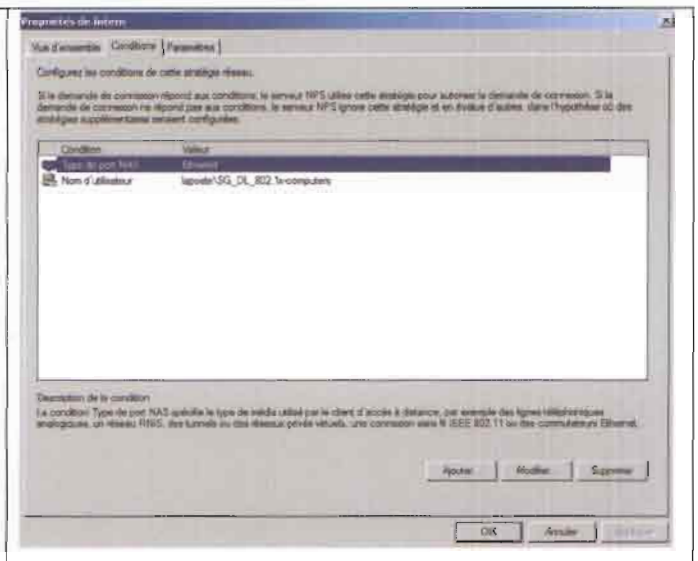
Ajouter la condition

NAS Port Type Ethernet

Et la condition **User Groups**

laposte\SG-DL-802.1x-Computers

qui correspond au groupe de sécurité contenant les ordinateurs de la société



Sous l'onglet **Contraints**

Choisir la catégorie

Authenticaton Methods

Ajouter à la liste, la méthode d'authentification

Microsoft : Smart Card or other certificate

qui correspond à une authentification

EAP-TLS

Cliquer sur **Edit**

et vérifier que le serveur

RADIUS se « présente »

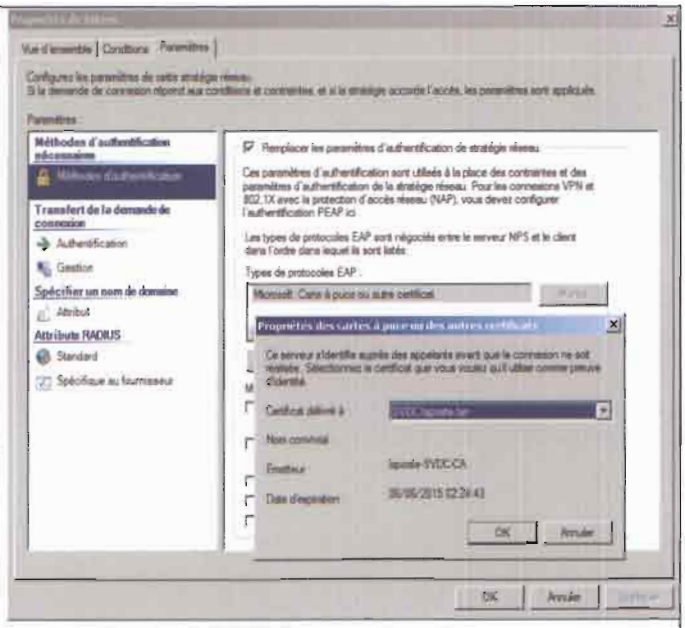
avec son certificat de domaine,

dans notre cas

SVDC.laposte.lan

Décocher toutes les autres

méthodes d'authentification



Sous l'onglet **Settings** et la

catégorie **Standard**

Ajouter les attributs suivants :

Framed-Protocol : PPP

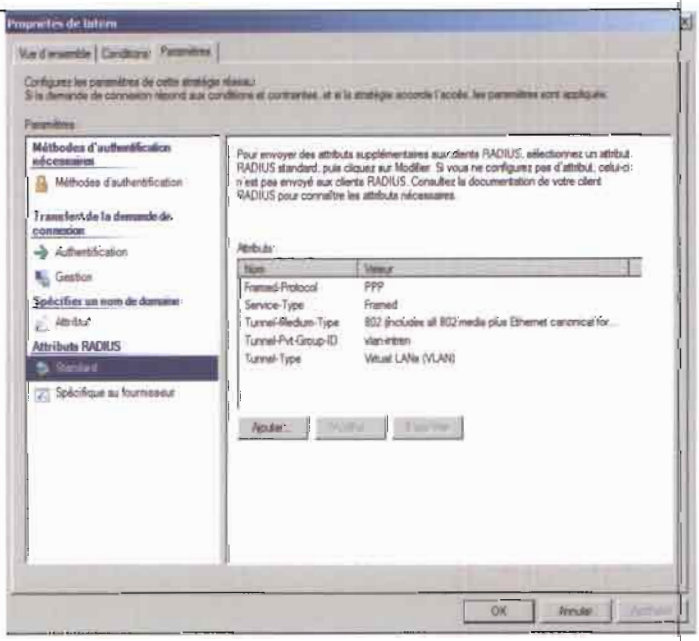
Service-Type : Framed

Tunnel-Medium-Type : 802

Tunnel-Type : Virtual Lans

Tunnel-Pvt-GroupID : VLAN-intern

Cette valeur correspond à l'assignation de VLAN et dans ce cas du VLAN-intern



(VLAN 2)	
L'attribut sous la catégorie **Vendor Specific** utilisé pour la Policy Voice est à retirer	

Logging & Accounting

Cette partie décrit la mise en place des mesures de traçage d'accès au réseau 802.1x.

Les serveur Syslog

Une solution très simple pour permettre un suivi des différents événements sur le Switch authentificateur 802.1x est la transmission des messages syslog du Switch vers un serveur syslog. Dans notre cas, nous avons opté pour le produit « Kiwi Syslog Server v9.1 » qui est installé en tant que service sur notre serveur SVDC. Nous avons choisi ce produit car il est simple d'utilisation, très complet et est en cours d'utilisation, en infrastructure de production du réseau d'entreprise actuel.

Configuration Switch

Commande	Description
logging 10.0.100.100	Active la transmission des syslog au serveur 10.0.100.100 (SVDC)

Configuration Kiwi Syslog Server

- **Règles**

Pour permettre un suivi plus efficace et pour pouvoir associer des actions à des messages syslog bien précis, nous devons configurer des règles :

Dans le menu setup du Kiwi Syslog Service Manager, nous avons ajouté une règle 802.1x Fails ;

Nous avons également ajouté un filtre **Only Dot1x and MAB** de catégorie **Message text** où filtrent sur les mots clés **DOT1X-5-FAIL** et **MAB-5-FAIL**

Ces mots clés peuvent être multiples, ils doivent être entourés par des guillemets et séparés par un espace (correspond à une OU implicite) ;

Nous avons ajouté une action **Display** de catégorie **Display** pour afficher le syslog filtré dans la fenêtre de Kiwi Syslog ;

Nous avons également ajouté l'action **Log to file** de type **Log to file** pour écrire le syslog dans un fichier texte ;

Nous avons aussi activé la rotation de fichier log pour créer un autre fichier lorsque l'ancien a atteint sa taille limite de **50 MB ;**

Enfin, la dernière action ajoutée est l'envoi de mail vers une adresse d'alerte **framicke@lapost.lan** en incluant comme message le syslog filtré

NB : Comme nous ne disposons pas de serveur mail de type exchange pour notre prototype, cette action ne pourra pas aboutir.

Elle remplit uniquement le rôle d'exemple.

Microsoft Event Viewer

L'outil intégré à chaque système d'exploitation Microsoft Windows, le Microsoft Viewer (MEV), permet un suivi complet de tous les événements sur un ordinateur ou serveur. Lors de l'ajout d'un rôle spécifique pour le serveur, une catégorie spéciale correspondant au rôle est créée dans l'event viewer.

Les informations qui nous permettent d'avoir un certain suivi sur les accès au réseau sont :

- **Les événements DHCP**
  - Permettant de voir les événements DHCP.
  - Malheureusement, ne permettent pas de voir l'historique des distributions d'adresses et des leases directement dans l'event viewer mais uniquement dans des fichiers log sous format texte.
- **Les événements NPS**

- Permettent de voir quels supplicants ont été autorisés à accéder le réseau et quels ont été refusés.

- Ne permettent pas de voir les connexions des supplicants Guest puisque l'accès au réseau Guest n'est pas géré par le service NPS mais par les Switches eux-mêmes.

Configuration

Aucune configuration de base n'est nécessaire puisqu'il s'agit d'une fonctionnalité intégrée à Windows Server 2008. Cependant, nous pouvons créer des actions pour des événements spécifiques pour envoyer un email d'alerte par exemple.

4.2.4 Les équipements réseau

1. Les ordinateurs de la SONAPOST

Installation

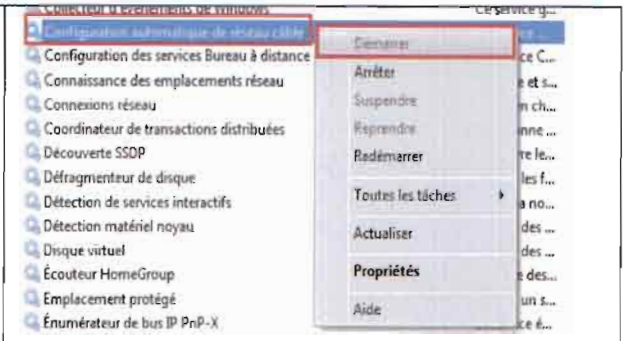
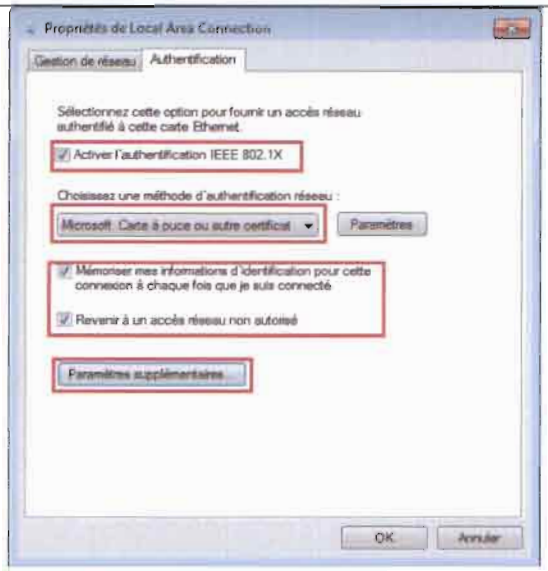
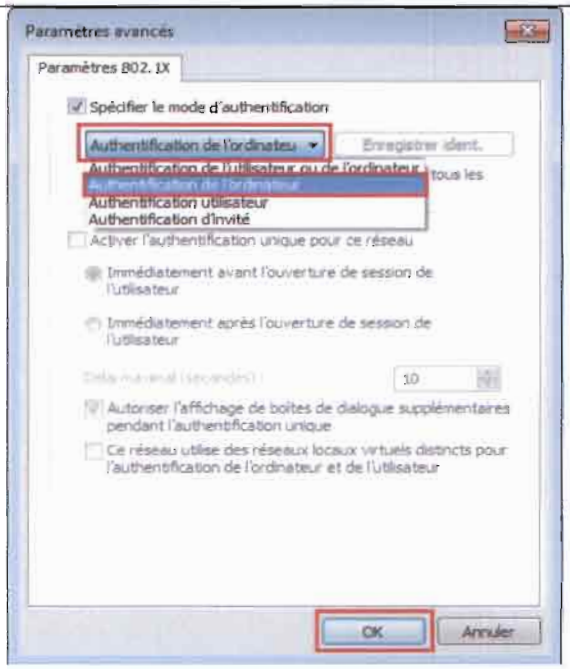
Installation Windows 7 Pro Standard et mise dans le domaine laposte.lan

Configuration

Ajout du certificat machine :

- Se connecter sur l'ordinateur cible avec un compte du domaine laposte.lan Lancer une console mmc Cliquer sur Fichier Puis Ajouter /Supprimer un composant logiciel enfichable
- Dans la nouvelle fenêtre, choisir **Certificats** puis Ajouter Choisir un compte d'ordinateur puis Suivant et Terminer Valider par OK
- Aller sur **Certificats** puis cliquer droit sur **Personnel** Choisir **Toutes les tâches** puis Demander un nouveau **certificat**
- Suivre l'assistant puis choisir **Ordinateur** valider par Inscription Attendre la fin du processus d'inscription

Activer la fonctionnalité 802.1x (sous Windows 7)

Démarrer le service Configuration automatique de réseau câblé	
Aller sur les paramètres de la carte réseau filaire Sous l'onglet authentification cocher **Activer l'authentification** **IEEE 802.1X** puis choisir **Microsoft : Carte à puce** **ou autre certificat** cocher les deux cases supplémentaires puis cliquer sur **Paramètres supplémentaire**	
Choisir dans la liste Authentification de l'ordinateur valider par OK	

4.3 Test du contrôle des accès

4.3.1 Scénario 1.1

Description du test	**Attente**	**Résultat**	**Visa**
Connexion d'un ordinateur d'entreprise présent dans le domaine et configuré correctement pour l'authentification EAP-TLS sur tous les types de ports 802.1x	Echec du processus MAB Réussite du processus dot1x Mis dans le VLAN 2	L'ordinateur NOHRMS075 est mis dans le VLAN 2 (Intern)	**OK**

Observations

```
*Mar 1 20:29:49.557: %AUTHMGR-5-START: Starting 'mab' for client (0017.a4cd.60df) on
Interface Gi0/1
*Mar 1 20:29:49.566: %MAB-5-FAIL: Authentication failed for client (0017.a4cd.60df) on
Interface Gi0/1
*Mar 1 20:29:49.566: %AUTHMGR-7-RESULT: Authentication result 'fail' from 'mab' for client
(0017.a4cd.60df) on Interface Gi0/1
*Mar 1 20:29:49.566: %AUTHMGR-7-FAILOVER: Failing over from 'mab' for client
(0017.a4cd.60df) on Interface
Gi0/1
*Mar 1 20:29:49.566: %AUTHMGR-5-START: Starting 'dot1x' for client (0017.a4cd.60df) on
Interface Gi0/1
*Mar 1 20:29:49.708: %DOT1X-5-SUCCESS: Authentication successful for client
(0017.a4cd.60df) on Interface Gi0/1
*Mar 1 20:29:49.708: %AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for
client
(0017.a4cd.60df) on Interface Gi0/1
*Mar 1 20:29:50.514: %AUTHMGR-5-SUCCESS: Authorization succeeded for client
(0017.a4cd.60df) on Interface Gi0/1
SW-C-000#show authentication sessions interface gigabitEthernet 0/1
Interface: GigabitEthernet0/1
PHYSIQUE Address: 0017.a4cd.60df
IP Address: Unknown
User-Name: host/NOHRMS075.tpi2010.local
Status: Authz Success
Domain: DATA
Oper host mode: multi-domain
Oper control dir: both
Authorized By: Authentication Server
VLAN Policy: 2
Session timeout: 3600s (local), Remaining: 3544s
Timeout action: Reauthenticate
Idle timeout: N/A
Common Session ID: 0A0064020000000330465EFF1
Acct Session ID: 0x00000041
Handle: 0x65000033
Runnable methods list:
Method State
mab Failed over
dot1x Authc Success
```

4.3.2 Scénario 1.2

Description du test	Attente	Résultat	Visa
Connexion d'un ordinateur externe sur tous les types de ports	Echec du processus MAB Echec du processus dot1x Application du VLAN guest Mis dans le VLAN 3	L'ordinateur externe est mis dans le VLAN 3 (Guest)	OK

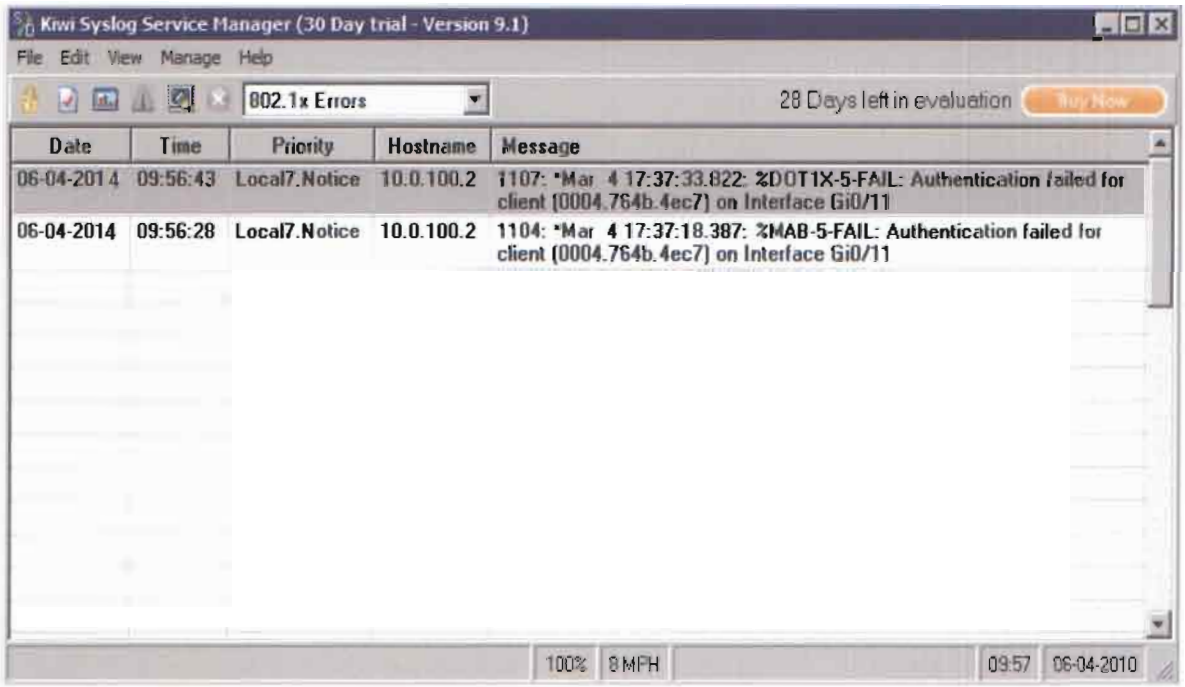
Observations

```
*Mar 1 20:35:46.232: %AUTHMGR-5-START: Starting 'mab' for client (0004.764b.4ec7) on
Interface Gi0/1
*Mar 1 20:35:46.241: %MAB-5-FAIL: Authentication failed for client (0004.764b.4ec7) on
Interface Gi0/1
*Mar 1 20:35:46.241: %AUTHMGR-7-RESULT: Authentication result 'fail' from 'mab' for client
(0004.764b.4ec7) on Interface Gi0/1
*Mar 1 20:35:46.241: %AUTHMGR-7-FAILOVER: Failing over from 'mab' for client
(0004.764b.4ec7) on Interface
Gi0/1
*Mar 1 20:35:46.241: %AUTHMGR-5-START: Starting 'dot1x' for client (0004.764b.4ec7) on
Interface Gi0/1
*Mar 1 20:36:01.684: %DOT1X-5-FAIL: Authentication failed for client (0004.764b.4ec7) on
Interface Gi0/1
*Mar 1 20:36:01.684: %AUTHMGR-7-RESULT: Authentication result 'no-response' from 'dot1x'
for client
(0004.764b.4ec7) on Interface Gi0/1
*Mar 1 20:36:01.684: %AUTHMGR-7-FAILOVER: Failing over from 'dot1x' for client
(0004.764b.4ec7) on Interface
Gi0/1
*Mar 1 20:36:01.684: %AUTHMGR-7-NOMOREMETHODS: Exhausted all authentication methods for
client
(0004.764b.4ec7) on Interface Gi0/1
*Mar 1 20:36:02.020: %AUTHMGR-5-SUCCESS: Authorization succeeded for client (Unknown
PHYSIQUE) on Interface
Gi0/1
SW-C-000#show authentication sessions interface gigabitEthernet 0/1
Interface: GigabitEthernet0/1
PHYSIQUE Address: Unknown
IP Address: Unknown
User-Name: UNRESPONSIVE
Status: Authz Success
Domain: DATA
Oper host mode: multi-host
Oper control dir: both
Authorized By: Guest VLAN
VLAN Policy: 3
Session timeout: N/A
Idle timeout: N/A
Common Session ID: 0A0064020000036046B55AC
Acct Session ID: 0x00000045
Handle: 0xCA000036
Runnable methods list:
Method State
mab Failed over
dot1x Failed over
```

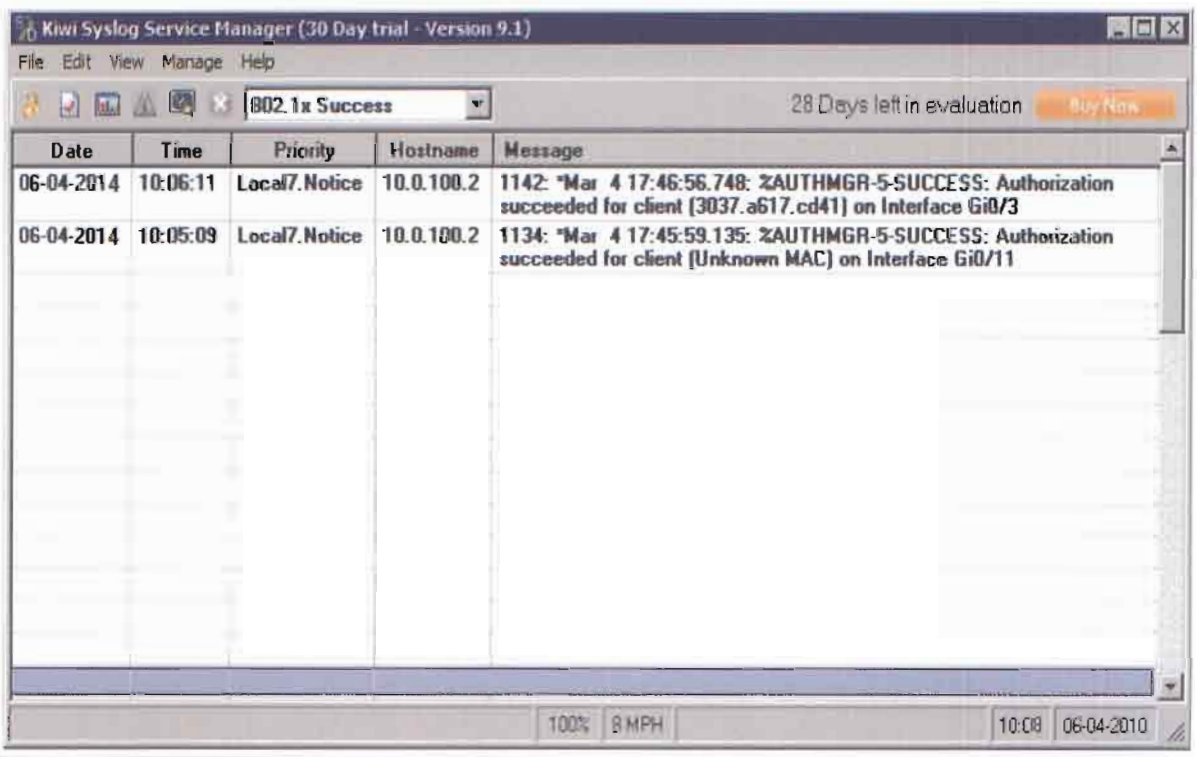
4.3.3 syslog

Une fois le Kiwi Syslog Server configuré correctement, nous pouvons voir arriver seulement les syslog concernant les requêtes dot1x ou mab

Requêtes échouées :



Requêtes avec succès :



V. Politique de mise en quarantaine

En matière de sécurité, dans le domaine des systèmes d'informations comme ailleurs, le plus dangereux est bien souvent de se reposer, consciemment ou non, sur une fausse assurance. Une démarche saine serait de gérer l'incertitude, de maintenir une inquiétude raisonnée et d'entretenir une véritable vigilance. Dans ce cadre, nous avons mené une étude consacrée à définir et à formaliser des concepts de sécurité applicable au domaine de la sécurité des systèmes d'information, afin de permettre le bon fonctionnement pratique et opérationnel en matière de contrôle d'accès aux ressources du système d'information et la gestion des risques lors de sa mise en fonction.

Nous considérerons ici les clients authentifiés et reconnus qui doivent avoir accès aux différentes ressources de la société. Ces clients dont la mobilité varie doivent faire l'objet d'un contrôle strict afin d'éviter une compromission de la sécurité du système d'information de la structure qui les héberge. Ce contrôle doit s'effectuer dans une zone réseau tampon : la zone de quarantaine. Dans cette dernière, les accès sont limités et n'autorisent que l'évaluation et les mises à jour logicielles (anti-virus, système d'exploitation,...). Nous avons adopté deux principales méthodes pour la mise en quarantaine.

La « quarantaine par VLAN dédié », consiste à cloisonner le client réseau dans un VLAN dédié dès sa demande de connexion. La procédure de mise en quarantaine est la suivante :

- Etape 1 : le client demande l'accès au réseau, via le point d'accès.
- Etape 2 : le serveur RADIUS contrôle l'accès et change l'assignation du port du NAS sur le VLAN de quarantaine.
- Etape 3 : le client réseau qui n'a accès qu'aux fonctionnalités proposées sur le VLAN de quarantaine est contrôlé et éventuellement mis à jour.

- Etape 4 : le client réseau est conforme à la politique informatique interne et la fin de la quarantaine est décrétée. Le serveur de quarantaine informe le point d'accès pour une nouvelle assignation de VLAN sur le port de connexion. Le client accède désormais au réseau local.

Le contrôle est effectué par le serveur de validation logiciel par le biais d'un agent installé sur le client réseau. Une fois connecté et authentifié, cet agent établit un dialogue avec le serveur de validation afin de vérifier que les prérequis nécessaires à la libération du client sont réunis. Ce contrôle s'effectuera en se basant sur la liste (non exhaustive) suivante : système d'exploitation (version et patchs correctifs), antivirus (présence et version de la base de définition virale à jour), logiciels (présence de logiciels non-conformes à la politique de l'établissement tels que Skype, p2p, bots, ...), analyse spécifique (analyse de certaines clefs du registre spécifique pour les clients Microsoft Windows). En ayant comme serveur de contrôle NPS dans sa fonctionnalité de NAP.

Quarantaine par filtrage

Dans l'hypothèse où l'utilisation d'une zone spécifique de quarantaine ne serait pas jugée pertinente, nous envisageons de limiter les accès du client au sein du VLAN sur lequel il est connecté. Cette limitation, des accès des clients non conformes à la politique informatique de l'établissement, s'opérera au moyen de listes de contrôles (ACLs). Ces dernières permettent en effet de définir, pour chaque port du NAS, des règles spécifiques de filtrage des paquets IP émis ou reçus par le client. Le client sera alors confiné dans une « quarantaine par filtrage » qui ne donnera accès qu'à certaines ressources. Cette solution permet également de s'affranchir des problèmes liés au changement d'adresse IP du client dans l'hypothèse où ce dernier n'utiliserait pas un service DHCP. La solution de quarantaine par filtrage est à privilégier car les clients sont très mobiles (intervenants extérieurs, personnels de l'entreprise itinérants, etc...) et un contrôle logiciel est difficilement applicable. En effet, le confinement de ces clients dès la demande de connexion garantit la sécurité des systèmes informatiques et ce, quelque soit le lieu de connexion au réseau. De même, il pourrait être envisagé de limiter le trafic entrant et/ou sortant sur certains postes clients.

Utilisation de la métrologie du LAN

Nous avons opté pour l'utilisation de la métrologie du LAN pour effectuer des contrôles. Cette solution est retenue en complément de l'utilisation des solutions propriétaires qui imposent l'installation d'agents sur les postes clients. Ce contrôle est opéré au moyen d'une sonde réseau liée au routeur de bordure, par vérification du trafic émis par le poste client. Cette proposition de réseau réactif s'appuie sur l'utilisation d'un échantillonnage des flux émis ou reçus par le client réseau durant sa session de connexion. L'utilisation du RADIUS et des tables de contrôles associées permettent de connaître le port de connexion physique d'un client sur le point d'accès. Cette information couplée à la détection du comportement du client ne respectant pas la politique de sécurité de la société entraînera sa bascule automatique dans la zone de quarantaine, via des scripts et des commandes SNMP.

Notre réseau est exclusivement composé de matériels HP, majoritairement compatibles avec le 802.1x. Les commutateurs d'ancienne génération non compatibles imposent l'utilisation d'une solution de localisation des postes clients reliés au réseau. Nous utilisons la base de données associée à Cacti afin d'avoir une base contenant les adresses IP de nos commutateurs ainsi que les noms de communauté SNMP permettant la lecture de la MIB SNMP.

Algorithme général

La méthode que nous avons choisie et développée, afin de pouvoir déterminer les anomalies de fonctionnement, se décline comme suit :

- L'analyse du trafic aux fins de référencement des serveurs et des services offerts sur le réseau. Ce processus est continu et il permet d'ajouter de nouveaux services pendant l'utilisation du système de contrôle des postes clients.

- Le filtrage des protocoles tels que le Netbios et ce afin d'éviter la multiplication des alertes. Concrètement, cette opération conduit à la désactivation de l'analyse des paquets ayant comme source et/ou destination le protocole désigné, pour un serveur donné répertorié.

- Après obtention de la liste des serveurs et/ou services, l'analyse du trafic permettant de repérer les incohérences ou le non-respect de la politique réseau présente quatre possibilités :

  - ✓ Trafic normal entre serveurs : un des services référencés correspond soit au port source, soit au port de destination du trafic ;
  - ✓ Trafic anormal entre serveurs : aucun des ports source et/ou destination n'est référencé dans la liste des services autorisés et validés. Dans ce cas, une alerte mail est adressée à l'administrateur. En effet, il ne saurait être question de couper l'ensemble des accès en basculant un serveur en quarantaine ;
  - ✓ Trafic normal entre client et serveur : les services auxquels accède le client (ports de destination selon le sens du trafic) sont référencés dans la liste des services autorisés et validés ;
  - ✓ Trafic anormal entre clients : les clients n'étant pas supposés offrir un service réseau, le trafic entre eux s'avère suspect. Dans ce cas le client est mis en quarantaine si l'on détecte du « scan » ou des échanges trop importants de données de type « illégal ».

L'architecture du futur système, représentée préalablement, prend en charge la gestion des identités et des habilitations de tous les utilisateurs identifiés de la forêt de laposte.lan. Les autres forêts englobent l'ensemble des ressources du Système d'Information de la SONAPOST mais limités (dans les structures) à un sous-ensemble de ces ressources.

Afin d'assurer la gestion centralisée du contrôle d'accès aux ressources, les trois forêts Windows seront connectées par une approbation sélective de forêt entrante en bidirectionnel avec la forêt de laposte.lan (méthode présente dans annexe VI). On se retrouve dans le cas d'une architecture d'approbation de forêt, où le système central provisionne les autres systèmes. Ces derniers se chargent eux-mêmes de provisionner les ressources de leurs domaines. Pour étendre

l'authentification à l'ensemble des forêts reliées par l'approbation de forêt, avec l'aide des domaines et des approbations Active Directory, nous procédons par une authentification sélective entre les forêts. Les approbations sélectives permettent aux administrateurs de bénéficier d'une plus grande souplesse lorsqu'ils prennent des décisions relatives aux contrôles d'accès à l'échelle de la forêt.

La gestion du contrôle d'accès réseau sera assurée par des serveurs NPS ; configurer en « Proxy RADIUS » aux seins des différents sites géographiques de la SONAPOST. Pour router les demandes d'accès entre les clients RADIUS (serveurs d'accès) et les serveurs RADIUS, qui authentifient les utilisateurs et les équipements réseau, il est accordé des autorisations en exécutant les opérations de gestion des comptes associées à la tentative de connexion.

Pour notre travail, nous avons d'abord dû nous intéresser au fonctionnement de 802.1X dans le détail, avant de pouvoir nous lancer dans l'expérimentation. Nous avons également dû chercher des produits qui utilisent ce concept et qui soient facilement implantables dans une topologie de laboratoire virtuel sur GNS3. Cela a été fructueux seulement pour deux des trois systèmes choisis au départ, nous pouvons donc affirmer maintenant que nous avons fait des choix un peu trop rapidement et que nous aurions dû passer plus de temps sur la phase de sélection des systèmes et de rassemblement de la documentation à leurs propos. Mis à part cet obstacle, ce travail de recherche et d'étude s'est déroulé comme prévu et nous a apporté beaucoup de nouvelles connaissances ainsi qu'un plaisir certain.

La mise en place de la nouvelle infrastructure de contrôle du système de contrôle ne demande pas l'achat de nouveaux équipements. Le tableau 9 ci-dessous nous donne une estimation des coûts.

Tableau 10: Evaluation des coûts

Désignation	Quantité	Prix unitaire (FCFA)	Prix total (FCFA)
Etude du système	02	16 500 000	33 000 000
Configuration de l'infrastructure	01	3 000 000	3 000 000
Formation des utilisateurs	01	1 500 000	1 500 000
Coût total	-	-	37 500 000

Perspectives

Le contrôle d'accès aux ressources internes est devenu un enjeu majeur pour les organismes. Nous avons présenté l'environnement et les solutions liées à un contrôle d'accès au réseau puis, nous avons décrit la solution de contrôle d'accès. Afin d'avoir une sureté du système d'information et un contrôle d'accès continue, la mise en quarantaine pour les clients réseaux équipés d'un agent logiciel fut nécessaire. Cette solution qui est l'une des plus abouties en terme de contrôle de poste client est la plus répandue. Le client qui ne respecterait pas la politique informatique de l'organisme ne pourrait prétendre à un accès aux ressources réseaux et services. En revanche, cette solution n'est pas applicable aux clients extérieurs par exemple. Cette restriction explique notre choix de solution d'analyse en temps réel des flux du client et de « pseudo-quarantaine » qui le confine au sein de son VLAN et/ou restreint ses accès à une liste prédéterminée de serveurs.

L'impact de cette nouvelle forme de quarantaine sur le fonctionnement du réseau est minime puisque pour chaque port analysé par un agent SFlow moins de 1/50 de trafic supplémentaire circule à destination du collecteur. Le seul aspect que nous intégrerons dans les perspectives de notre recherche sera de limiter le nombre d'ACLs par le point d'accès, afin d'éviter que la charge CPU ne devienne trop importante. Une analyse approfondie et automatisée des flux nous permettra de mieux déterminer le comportement à risque d'un client du réseau. Les réponses

seront soit une mise en quarantaine simple (protégée par un portail captif), soit une quarantaine filtrée (utilisation d'ACLs), soit enfin une quarantaine cloisonnée (basculement dans un VLAN dédié). En complément de l'analyse des flux, nous envisageons d'utiliser le logiciel OCS Inventory comme agent libre de contrôle logiciel afin de disposer, dans notre schéma de gestion de la quarantaine, de l'ensemble des moyens de supervision des clients. Par ailleurs, la localisation physique précise d'un client, pourrait être obtenue en couplant les informations recueillies lors de l'authentification avec celles issues d'une base de données géographiques.

Conclusion

L'étude détaillée de la solution et la réalisation du prototype, nous ont permis de connaitre tous les détails du système. Aussi, cela nous a permis de comprendre le fonctionnement du système de contrôle d'accès. Au terme de ce chapitre, nous pouvons décrire les phases de transition, ainsi que le matériel requis et donner la certitude du bon fonctionnement du système de contrôle d'accès d'un tel système.

Le contrôle d'accès aux ressources du système d'information est l'une des principes de la sécurité des systèmes d'information en pleine expansion. Il est clair et évident que l'un des avantages principaux du système de contrôle centralisé est la réduction du coût d'administration et de gestion interne de la sécurité. Par conséquent, la mise en place d'une solution de contrôle d'accès est d'une nécessité importante pour réduire le problème de sécurité au sein de la SONAPOST.

A cet effet, notre étude nous a amené à proposer une solution de contrôle d'accès logique. Cette solution implique la mise en place d'un système d'authentification au sein des zones sensibles du système. Ce dernier est l'agrégation de la gestion des identités et des habilitations des utilisateurs et du contrôle des accès réseau. Ceux-ci avaient pour buts respectifs de donner une vue de l'ensemble des utilisateurs et des équipements du système ayant chacun un identifiant unique dans le système et doté des droits bien spécifiques sur les ressources du système ; de pouvoir authentifier tout utilisateur du système et vérifier quel type de droits il possède sur la ressource à laquelle il veut accéder. La réalisation de tout ce mécanisme passe par trois services que nous avons définis suivant les fonctionnalités que nous voulons. Il s'agit du service annuaire que nous avons utilisé pour le stockage et la gestion des identités et des habilitations, les serveurs d'authentification avec les protocoles authentification et les systèmes d'authentification. C'est à la suite de cette étude que nous avons proposé une architecture fonctionnelle en vue de donner la représentation de notre solution et de son modèle d'intégration suivant notre système informatique à la SONAPOST.

Au terme de cette étude, nous retiendrons que l'élaboration de ce document nous a permis, d'une part d'approfondir nos connaissances acquis durant notre formation, et d'autre part de préparer notre intégration dans la vie professionnelle.

I. Liste des ressources du système d'information à protéger

Le tableau ci-dessous représente les ressources informatiques du système d'information

Nature	Ressources	Niveau d'importance	Accessibilité/utilisateur (ou exploitant)	Localité
Physique	Serveurs	Très	Peu / Administrateur système	Salle serveur
	Routeurs	Très	Peu / Administrateur système	Salle serveur
	Switchs	Pas trop	Peu / Administrateur système	Salle serveur Rack
	Ordinateurs	Pas trop	Très / Utilisateur	Bureau de service
	Imprimante	Pas trop	Très / Utilisateur	Bureau de service
	Téléphone IP	Pas trop	Très / Utilisateur	Bureau de service
	Caméras de surveillance	Pas trop	Très peu / service maintenance	Recoins des immeubles
	Prises informatiques	peu	Très peu / service maintenance et utilisateur	Bureau de service
	câbles de connexion	peu	Très peu / service maintenance	Encastré dans le mur
	Cordon de	Peu	Très / Utilisateur	Entre l'ordinateur et

	connexion			la prise informatique
Logique (numérique)	Bases de données	Très	Très / administrateurs	Serveur de bases des données
	Application	Très	Très / utilisateur	Serveur d'application
	Fichiers partagers	Très	Très / utilisateur	Serveur de fichiers
	Système d'exploitation	Très	Très / utilisateur et Administrateur	Dans serveurs et ordinateurs

II. Etude de Modèle Base Access Control (RBAC)

Le modèle de sécurité RBAC (Role Based Access Control) est principalement issu d'Internet afin de prendre en compte des applications déployées sur de vastes organisations ou des applications inter-organisations (Extranet par exemple). Ce modèle permet en particulier de simplifier l'administration des droits et de prendre en compte la délégation de l'administration. Les concepts du RBAC ont servi de base à la norme établie par American National Standard et référencée sous le N°:ANSI INCITS 359-2004 (approuvée le19 Février 2004). Ce modèle tend à se généraliser dans l'industrie et un nombre croissant de produits supporte un modèle d'habilitation "orienté rôles".

Le modèle RBAC se distingue du modèle DAC (Discretionary Access Control) popularisé par Unix. Le modèle DAC est centré sur les ressources physiques (fichier, exécutable, etc.) et identifie un propriétaire ainsi que des groupes d'utilisateurs ayant des droits sur la ressource (lecture, écriture, etc.). Le modèle RBAC modélise des fonctions métiers plutôt que des accès à des ressources informatiques. Un rôle correspond à une fonction au sein d'une organisation. Le principe de base du RBAC est que deux utilisateurs ayant les mêmes rôles ont les mêmes droits sur le système. L'administration des rôles est ainsi facilement compréhensible par des

administrateurs métiers et peut être déléguée. Les associations entre les rôles et les ressources physiques sont modélisées séparément par les concepteurs d'application et le maîtrise d'ouvrage métier.

Le standard propose un modèle de base (Core RBAC) ainsi que les extensions présentées au-dessus. Les concepts manipulés par le modèle RBAC sont les suivants :

- USERS (Utilisateurs) : comptes permettant aux utilisateurs de se connecter au système,
- ROLES (Rôles) : fonctions métiers dans des organisations ou des périmètres donnés (par exemple : vendeur résidentiel dans l'agence X),
- OBS (Objets) : objets informatiques à protéger,
- OPS (Opérations) : opérations possibles sur les objets,
- PRMS (Permissions) : autorisation d'effectuer l'opération X sur l'objet Y,
- SESSIONS (Sessions) : session temporelle, chaque session est associée à un utilisateur pour une période de temps limitée,
- un utilisateur possède un rôle sur un périmètre donné,
- un rôle donne droit à des permissions,
- une permission est un ensemble d'opérations sur un objet,
- le contrôle d'accès se déroule au cours d'une session,
- au cours d'une session, il peut être nécessaire qu'un utilisateur n'ait qu'un et un seul rôle. C'est la notion de rôle actif,
- le périmètre est porté par un rôle et il est transmis de manière aveugle à l'application (la permission).

Note : le rôle est généralement accompagné par un périmètre (par exemple le numéro de compte client). La sémantique du périmètre est propre à l'application et n'est généralement pas contrôlée par le système de contrôle d'accès. Cette information est toutefois renseignée au cours du processus de déclaration des droits

et participe pleinement aux contrôles de sécurité faits par l'application. Le système de contrôle d'accès joue simplement le rôle de courtier pour cette information.

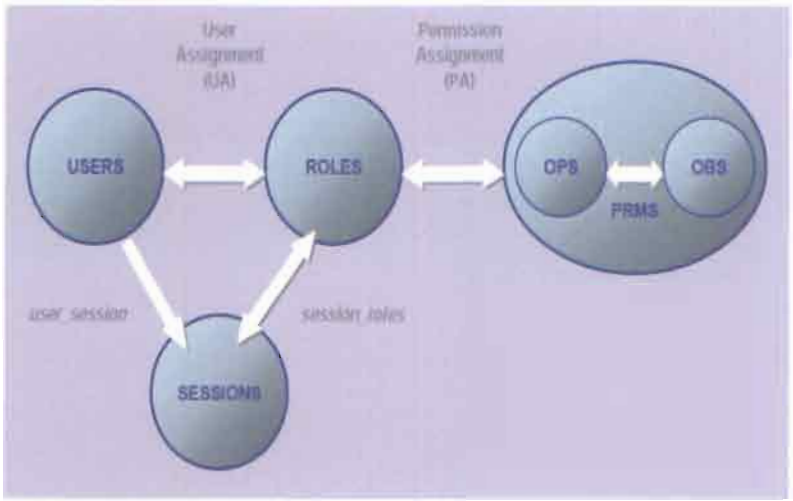


Figure : Modèle de base RBAC

Le fonctionnement de ce modèle et l'intégrité du système sont garantis si l'attribution des permissions respecte le principe de privilège minimum. Ce principe exige que l'utilisateur ne dispose pas de plus de droits que nécessaire à son travail. Ce qui implique que les permissions affectées à un rôle constituent le strict minimum nécessaire à l'accomplissement des tâches relatives à ce rôle.

- **Modèle RBAC Hiérarchique**

Le modèle RBAC hiérarchique (Hierarchical RBAC) ajoute au modèle de base le support de hiérarchie des rôles. La hiérarchie établit les liens de parenté entre plusieurs niveaux des rôles et permet aux rôles « parents » de disposer des permissions attribuées aux rôles « enfants ». Le standard admet deux types de hiérarchies :

- le modèle hiérarchique général (General Hierarchical RBAC) : cette variante établi des relations multiples entre plusieurs « parents » et « enfants »,
- le modèle hiérarchique limité (Limited Hierarchical RBAC) : cette version limite la relation à une simple structure d'arborescence. Ce qui veut dire qu'un rôle ne peut avoir qu'un seul « parent ».

Cette extension du modèle permet une administration plus efficace dans les grandes

structures qui gèrent de très nombreuses permissions d'un grand nombre d'utilisateurs.

Ce principe permet de bien gérer les situations où certains rôles différents (du niveau supérieur) doivent bénéficier de certaines permissions communes.

Remarque : Très souvent, nous appliquons une version simple de l'extension au modèle hiérarchique limité. Elle admet une hiérarchie des rôles à deux niveaux. Le niveau 1 est appelé « un rôle » et le terme d'« un profil » sera utilisé pour le deuxième niveau. Le profil permettra donc les regroupements des rôles.

- **Modèle RBAC avec contraintes**

Le modèle RBAC avec contraintes (Constrained RBAC) ajoute au modèle la contrainte de séparation des pouvoirs. Cette contrainte permet d'inclure dans le modèle, la gestion de conflits d'intérêts et de s'assurer que les utilisateurs bénéficieront des permissions selon la politique définie par l'organisation. Les utilisateurs ne pourront pas abuser de cumul non contrôlé de droits.

- **Séparation Statique des Pouvoirs (SSD - Static Separation of Duty Relations)**

La contrainte de séparation des pouvoirs est utilisée pour assurer le respect de la politique des habilitations. Un conflit d'intérêts peut arriver (dans un système du type RBAC) quand l'utilisateur obtient simultanément les droits associés à des rôles incompatibles. Une méthode pour éviter cette situation est la mise en œuvre de séparation statique de pouvoir (SSD pour Static Separation of Duty).

L'exclusion mutuelle de certains rôles est spécifiée par les règles de SSD. Ces règles sont interprétées lors du processus d'affectation des rôles par l'administrateur et l'empêchent d'affecter des rôles incompatibles au même utilisateur. De cette manière, à une personne qui bénéficie d'un rôle. Il sera impossible d'affecter un deuxième rôle interdit par la règle de SSD. Pour éviter les incohérences, les règles SSD doivent prendre en compte les regroupements des rôles en fonction de leur hiérarchie.

- **Séparation Dynamique des Pouvoirs (DSD - Dynamic Separation of Duty Relations)**

La séparation dynamique limite, comme la SSD, les rôles accessibles à un utilisateur. Par contre le contexte est différent. La limitation n'est pas exploitée au moment de l'affectation des rôles mais au moment de leur activation dans une session.

Dans une même session, un utilisateur a la possibilité de ne pas activer tous ses rôles, mais uniquement le sous-ensemble de ses rôles nécessaires à la réalisation de la tâche à accomplir. Ce mécanisme permet de garantir l'application des permissions minimales nécessaires dans une période d'exécution d'une tâche. On peut parler, dans ce contexte, de révocation temporaire des privilèges. La mise en œuvre de ce mécanisme peut se révéler très complexe et le plus souvent irréalisable.

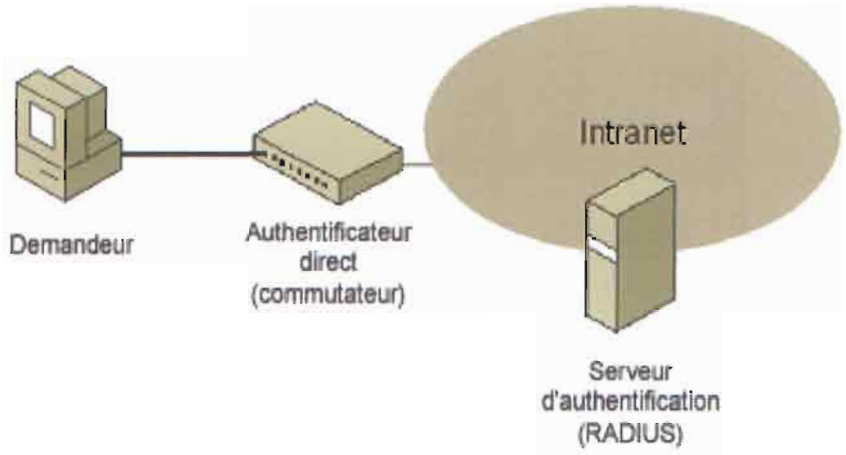
II. La norme 802.1X

La norme IEEE 802.1X définit un contrôle de l'accès réseau basé sur le port. Elle permet un accès réseau authentifié pour les réseaux filaires et sans fil. Le contrôle d'accès réseau basé sur le port s'appuie sur les caractéristiques physiques d'un réseau local commuté pour authentifier les équipements attachés à un port sur ce réseau. L'utilisation du port est refusée si le processus d'authentification échoue. Le port peut également être assigné à un VLAN qui ne contient pas de ressources sensibles.

➢ Éléments de 802.1X

IEEE 802.1X définit les éléments suivants :

1. Le demandeur (en anglais : *supplicant*)
2. L'authentificateur direct (en anglais : *pass-through authenticator*)
3. Le serveur d'authentification



La figure montre ces éléments dans un réseau filaire.

Figure 1- Les éléments de l'authentification IEEE 802.1X pour des réseaux filaires.

- **Demandeur**

Le demandeur est un ordinateur qui demande l'accès à un réseau via l'authentificateur direct. Pour les connexions filaires, le demandeur est un ordinateur équipé d'une carte réseau, physiquement attaché à un port commuté, qui demande l'accès à l'intranet.

- **Authentificateur direct**

L'authentificateur direct est le commutateur qui met en œuvre l'authentification avant d'autoriser l'utilisation des ports du réseau local (LAN) du commutateur. En règle générale, l'authentificateur direct n'effectue pas lui-même l'authentification et l'autorisation. Il passe les informations d'authentification fournies par le demandeur ainsi que d'autres informations de connexion à un serveur d'authentification.

- **Serveur d'authentification**

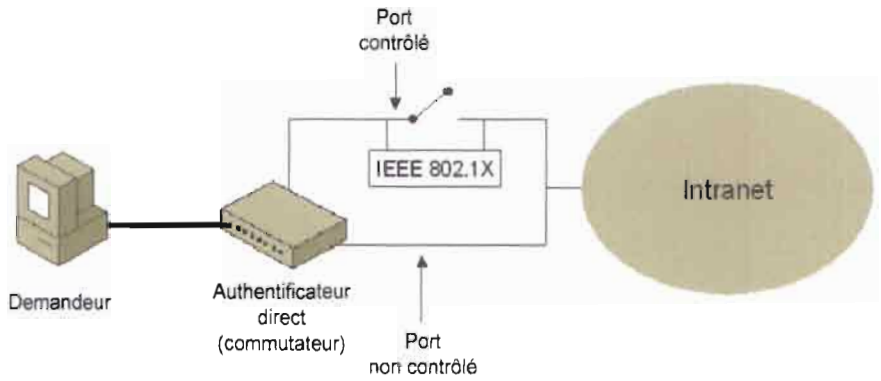
Le serveur d'authentification authentifie et autorise une tentative de connexion de la part de l'authentificateur direct. Il valide les informations d'authentification du demandeur, évalue l'autorisation de la tentative de connexion et répond à l'authentificateur direct en indiquant si le demandeur est autorisé à se connecter. Le serveur d'authentification peut être un des éléments suivants :

- Un composant du commutateur. Dans ce cas, le commutateur doit être configuré avec les éléments d'informations d'authentification de l'utilisateur qui correspondent aux demandeurs autorisés et aux stratégies d'autorisation. Cette implémentation est rarement utilisée en raison de l'absence de gestion centralisée et des problèmes de montée en charge.
- Un ordinateur individuel sur l'intranet. Dans ce cas, le commutateur transfère les informations d'authentification de la tentative de connexion au serveur d'authentification. Ceci décrit comment un commutateur peut utiliser le protocole RADIUS (Remote Authentication Dial-In User Service) pour envoyer un message de demande de connexion à un serveur RADIUS.

➢ Ports contrôlés et non contrôlés

IEEE 802.1X définit les types de ports logiques suivants qui accèdent à un intranet via un port LAN physique unique :

- **Port non contrôlé** : Il permet à l'authentificateur direct de communiquer avec d'autres nœuds sur l'intranet (tels que le serveur d'authentification). Les trames envoyées par les demandeurs ne sont jamais envoyées à l'aide du port non contrôlé.
- **Port contrôlé** : Il permet à un demandeur d'échanger des trames avec les nœuds sur l'intranet, uniquement si le demandeur est authentifié et autorisé par 802.1X. Avant l'authentification et l'autorisation, le port contrôlé est bloqué et aucune trame ne circule entre le demandeur et l'intranet. Lorsque le demandeur est authentifié et autorisé, le port s'ouvre et les trames peuvent circuler entre le demandeur et les nœuds sur l'intranet.



La figure montre les différents types de ports.

Sur un commutateur Ethernet d'authentification, le client Ethernet commuté peut envoyer des trames Ethernet à l'intranet dès que l'authentification et l'autorisation sont terminées. Le commutateur identifie le trafic pour un demandeur donné via le port physique auquel le demandeur est connecté.

Pour fournir un mécanisme d'authentification standard pour les connexions authentifiées 802.1X, l'IEEE a choisi le protocole EAP (Extensible Authentication Protocol). EAP est un mécanisme d'authentification basé sur le protocole PPP (Point-to-Point Protocol) qui a été adapté pour une utilisation sur des segments LAN point à point. Pour les connexions PPP, les messages EAP sont envoyés sous la forme de charges dans des trames PPP. Pour adapter les messages EAP afin qu'ils soient envoyés sur des segments LAN Ethernet, la norme IEEE 802.1X définit EAPOL (EAP over LAN), une méthode d'encapsulation standard pour les messages EAP.

- **Présentation d'EAP**

EAP est une extension de PPP créée pour permettre le développement de méthodes d'authentification d'accès réseau. Avec les protocoles d'authentification PPP standards, un mécanisme d'authentification spécifique est choisi lors de la phase d'établissement de la liaison de la connexion PPP. Lors de cette phase d'authentification de la connexion PPP, le protocole d'authentification PPP négocié est utilisé pour authentifier la connexion à l'aide d'une série de messages fixes dans un ordre spécifique.

Avec EAP, le mécanisme d'authentification spécifique n'est pas choisi lors de la phase d'établissement de la liaison de la connexion PPP. À la place, chaque

homologue PPP utilise le protocole EAP lors de la phase d'authentification de la connexion. Lorsque la phase d'authentification de la connexion est atteinte, les homologues négocient l'utilisation d'un schéma d'authentification EAP spécifique appelé type EAP. Une fois le type EAP accepté, EAP autorise l'échange libre de messages entre le demandeur et le serveur d'authentification (le serveur RADIUS). La conversation se compose des demandes d'informations d'authentification et des réponses. La longueur et les détails de la conversation d'authentification dépendent du type EAP. EAP est décrit dans la RFC 3748.

Du point de vue de l'architecture, EAP permet l'utilisation de modules additionnels d'authentification sur le demandeur et sur le serveur d'authentification. Pour ajouter une prise en charge d'un nouveau type EAP, il suffit d'installer un fichier de bibliothèque de types EAP sur le demandeur et le serveur d'authentification. Cette extensibilité permet de fournir un nouveau schéma d'authentification à tout moment. EAP fait ainsi preuve d'une grande flexibilité pour permettre des méthodes d'authentification plus sécurisées.

Vous pouvez utiliser EAP, pour prendre en charge des schémas d'authentification qui autorisent différents niveaux de sécurité, tels que Generic Token Card, One Time Password (OTP), MD5-Challenge, Transport Layer Security (TLS) pour la prise en charge de cartes à puce et de certificats, ainsi que les futures technologies d'authentification. EAP est un composant fondamental pour sécuriser les connexions.

De plus, pour la prise en charge au sein de PPP, IEEE 802.1X définit la façon dont EAP est utilisé pour l'authentification par des périphériques IEEE 802, notamment les commutateurs Ethernet et les points d'accès sans fil IEEE 802.11. À la différence de PPP, IEEE 802.1X ne prend en charge que les méthodes d'authentification EAP.

- **EAP over RADIUS**

EAP over RADIUS n'est pas un type EAP, mais le passage de messages EAP, d'un type EAP quelconque, par l'authentificateur direct à un serveur RADIUS pour authentification. Un message EAP envoyé du demandeur à l'authentificateur direct est formaté comme attribut RADIUS EAP-Message (RFC 2869, section 5.13) et

envoyé dans un message RADIUS de l'authentificateur direct au serveur RADIUS. L'authentificateur direct passe les messages EAP entre le demandeur et le serveur RADIUS. Le traitement des messages EAP a lieu sur le demandeur et sur le serveur RADIUS, et non sur l'authentificateur direct, comme indiqué à la figure 3.

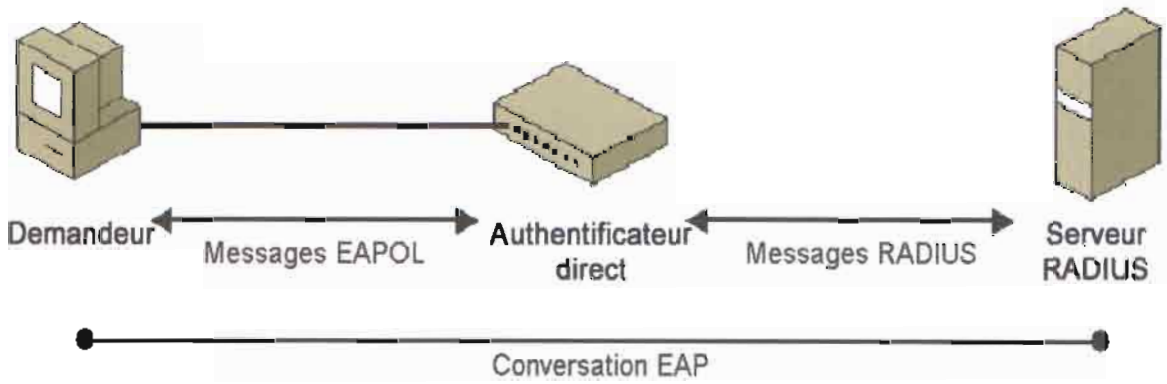


Figure 3. EAP over RADIUS.

EAP over RADIUS est utilisé dans des environnements où RADIUS est utilisé pour l'authentification, l'autorisation et la comptabilité (AAA, *Authentication, authorization, and accounting*). L'un des avantages de l'utilisation d'EAP over RADIUS est que les types EAP n'ont pas besoin d'être installés sur chaque authentificateur direct, mais uniquement sur le serveur RADIUS. Cependant, l'authentificateur direct doit prendre en charge EAPOL, la négociation initiale d'EAP et le transport des messages EAP vers un serveur RADIUS.

Dans une utilisation classique d'EAP over RADIUS, l'authentificateur direct est configuré pour utiliser EAP et RADIUS pour l'authentification, l'autorisation et la comptabilité. Lors d'une tentative de connexion, le demandeur négocie l'utilisation d'EAP avec l'authentificateur direct. Lorsque le client envoie un message EAP à l'authentificateur direct à l'aide d'EAPOL, l'authentificateur direct encapsule le message EAP en tant qu'attribut EAP-Message d'un message Access-Request RADIUS, et l'envoie au serveur RADIUS configuré. Le serveur RADIUS traite le message EAP dans l'attribut EAP-Message et envoie un message de réponse EAP sous la forme d'un message Access-Challenge RADIUS avec l'attribut EAP-Message à l'authentificateur direct. L'authentificateur direct transmet ensuite ce message EAP au demandeur à l'aide d'EAPOL.

- Avant et pendant l'authentification 802.1x, tout le trafic excepté les paquets EAPoL est bloqué en attendant l'authentification.

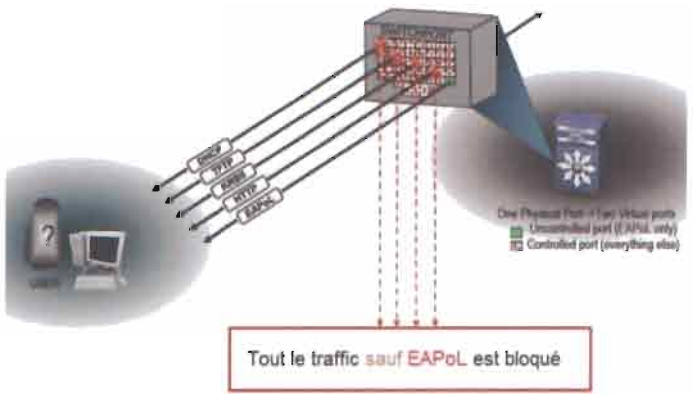


Figure avant / pendant l'authentification 802.1x

- Après une authentification positive, le port passe à un état ouvert permettant de véhiculer les paquets réseau.

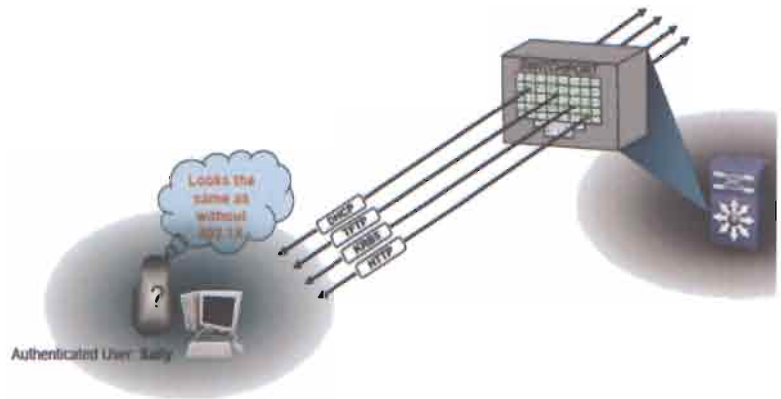


Figure après l'authentification 802.1x positive

Les connexions filaires peuvent utiliser les types EAP suivants :

- **EAP-Message Digest 5-Challenge Handshake Authentication Protocol (MD5-CHAP)** Un protocole simple qui utilise un nom d'utilisateur ou d'ordinateur et un mot de passe avec un mécanisme de hachage comme informations d'authentification. EAP-MD5-CHAP peut faire l'objet d'une attaque par dictionnaire hors ligne et n'est pas recommandé.
- **Protected EAP (PEAP)-Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2)** L'association d'un canal TLS chiffré (créé par PEAP) et d'un protocole challenge-handshake d'authentification mutuelle, qui utilise un nom

d'utilisateur et un mot de passe comme informations d'authentification. En raison du canal TLS, PEAP-MS-CHAP v2 n'est pas aussi sensible à une attaque par dictionnaire hors ligne. Pour effectuer une authentification TLS à sens unique pour PEAP, les serveurs RADIUS doivent disposer de certificats d'ordinateur auxquels les demandeurs accordent leur confiance. Au moment de la rédaction de ce document, PEAP-MS-CHAP v2 est la méthode EAP recommandée pour les informations d'authentification par nom d'utilisateur et mot de passe.

- **EAP-TLS** est une méthode d'authentification mutuelle bidirectionnelle utilisant TLS et des certificats numériques. EAP-TLS requiert une infrastructure de clés publiques (PKI) pour émettre et renouveler les certificats utilisateur ou d'ordinateurs, des ordinateurs demandeurs et les certificats d'ordinateurs des serveurs RADIUS.
- **PEAP-TLS** : L'association d'un canal TLS chiffré (créé par PEAP) et d'une méthode d'authentification mutuelle bidirectionnelle qui utilise TLS et des certificats numériques. Tout comme EAP-TLS, PEAP-TLS requiert une infrastructure de clés publiques (PKI) pour émettre et renouveler les certificats utilisateur ou d'ordinateurs des ordinateurs demandeurs et les certificats d'ordinateurs des serveurs RADIUS.

Les autorisations NTFS

Le système de fichiers NTFS (Windows NT File System) de Microsoft Windows 2008 permet de stocker très efficacement des données sur une partition. Ainsi, vous pouvez accorder des autorisations d'accès sur les dossiers et les fichiers afin de contrôler le niveau d'accès aux ressources dont bénéficient les utilisateurs. En outre, il permet de crypter des données de fichier sur le disque dur physique à l'aide du système de cryptage de fichiers EFS (Encrypting File System).

Les autorisations NTFS ne sont disponibles que sur les partitions NTFS. Pour sécuriser des fichiers et des dossiers sur des partitions NTFS, des autorisations NTFS doivent être accordées pour chaque compte d'utilisateur ou groupe d'utilisateurs qui veut accéder à la ressource. Les utilisateurs bénéficient d'une autorisation explicite pour pouvoir accéder aux ressources. Si aucune autorisation n'est accordée, le compte d'utilisateur ne peut pas accéder au fichier ou au dossier. Le système NTFS stocke une liste de contrôle d'accès ACL (Access Control List) associée à chaque fichier et dossier contenus dans une partition NTFS. La liste ACL

contient tous les comptes d'utilisateur, groupes et ordinateurs bénéficiant de l'accès au fichier ou au dossier, ainsi que le type d'accès qui leur est accordé.

➢ AUTORISATIONS NTFS SUR LES DOSSIERS

Le tableau suivant énumère les autorisations NTFS standards qui peuvent être accordées sur les dossiers et le type d'accès offert par chaque autorisation.

Autorisation NTFS sur les dossiers	**Possibilités offertes à l'utilisateur**
Lecture	Afficher les fichiers et les sous-dossiers contenus dans le dossier ainsi que les attributs, l'appropriation et les autorisations associées au dossier.
Ecriture	Créer des fichiers et des sous-dossiers dans le dossier, modifier les attributs du dossier et afficher l'appropriation et les autorisations associées au dossier.
Afficher le contenu du dossier	Afficher le nom des fichiers et des sous-dossiers contenus dans le dossier.
Lecture et exécution	Parcourir les dossiers et effectuer les opérations permises par les autorisations Lecture et Afficher le contenu du dossier.
Modifier	Supprimer le dossier et effectuer les opérations permises par les autorisations Ecriture, et Lecture et exécution.
Contrôle total	Modifier les autorisations, prendre possession d'un dossier, supprimer des sous-dossiers et des fichiers , et effectuer les opérations permises par toutes les autres autorisations NTFS sur les dossiers.

➢ AUTORISATIONS NTFS SUR LES FICHIERS

Le tableau suivant énumère les autorisations NTFS standards, pouvant être accordées sur les fichiers et le type d'accès offert par chaque autorisation.

Autorisation NTFS sur les fichiers	**Possibilités offertes à l'utilisateur**
Lecture	Lire le fichier et afficher les attributs, l'appropriation et les autorisations associés au fichier.
Écriture	Remplacer le fichier, modifier les attributs du fichier et afficher l'appropriation et les autorisations associées au fichier.
Lecture et exécution	Exécuter des applications et effectuer les opérations permises par l'autorisation Lecture.
Modifier	Modifier et supprimer le fichier et effectuer les opérations permises par les autorisations Ecriture, et Lecture et exécution.
Contrôle total	Modifier les autorisations, prendre possession d'un fichier et effectuer les opérations permises par toutes les autres autorisations NTFS sur les fichiers.

V. Politique de sécurité adoptée au réseau

1. Définitions des stratégies de sécurité

Nous définissons les stratégies de sécurité et des zones de sécurité

- **Stratégie des périmètres de sécurité**

L'objectif est de découper le réseau informatique de la SONAPOST en périmètres de sécurité logiques regroupant des entités ou fonctions afin de mettre en place des niveaux de sécurité à la fois imbriqués et séparés. Cependant, cette stratégie n'est pas suffisante et doit être couplée avec celle des goulets d'étranglement.

- **Stratégie des goulets d'étranglement**

L'objectif est de définir des contrôles d'accès différenciés et en nombre limité pour permettre l'accès à chaque périmètre de sécurité du réseau intranet. Les contrôles d'accès définissent ce qu'il est autorisé de faire pour entrer dans un périmètre de sécurité du réseau. Tout ce qui n'est pas autorisé est interdit et les contrôles d'accès définissent les conditions à respecter pour avoir le droit d'entrer dans un périmètre donné. Maintenant que les périmètres sont définis ainsi que les goulets d'étranglement, attelons-nous à authentifier les utilisateurs du réseau.

- **Stratégie d'authentification en profondeur**

L'objectif est de mettre en place des contrôles d'authentification pour authentifier les accès aux périmètres de sécurité. Pour ce faire, nous installons des systèmes de contrôle d'authentification au sein d'un périmètre qui leur est réservé.

- **Stratégie du moindre privilège**

Cette stratégie a pour objectif de s'assurer que chacun dispose uniquement des privilèges dont il a besoin. La portée de tout acte de malveillance s'en retrouve réduite aux privilèges dont dispose la personne qui le commet et il faudra une complicité de plusieurs personnes pour pouvoir mettre en péril le réseau intranet.

Un moyen simple de renforcer cette stratégie est d'augmenter les autorisations nécessaires pour accéder à une ressource.

- **Stratégie de confidentialité des flux réseau**

L'objectif de cette stratégie est de protéger tout message qui doit être émis vers un autre réseau ou Internet.

- **Stratégie de séparation de pouvoirs**

L'objectif est de créer des entités séparées, chacune responsable de zones de sécurité distinctes du réseau intranet.

- **Stratégie d'accès au réseau local :**

L'objectif de cette stratégie est d'assurer qu'aucune porte dérobée interne ne permette d'accéder au cœur du réseau. Pour contourner ce risque, il faut créer un contrôle d'accès à toutes les portes d'entrée du périmètre de sécurité.

- **Stratégie d'administration sécurisée**

L'objectif de cette stratégie est de créer une zone d'administration dédiée et séparée du réseau afin d'assurer une isolation des systèmes chargés de l'administration de chaque périmètre de sécurité. Une zone d'administration est en charge de vérifier le bon fonctionnement

- **Stratégie des Mots de passe**

L'utilisation de mots de passe par défaut ne doit pas être autorisée. La mise en vigueur des mots de passe comprenant un mélange de lettres majuscules et minuscules et des chiffres.
Le mot de passe doit contenir au moins 8 caractères.
L'utilisation de mots de passe semblables au nom de l'utilisateur ne doit pas être autorisée.

La mise en vigueur d'une politique de remplacement régulier du mot de passe. La fréquence de remplacement du mot de passe doit être basée sur le profil de risque, mais doit être effectuée au moins une fois tous les trois mois

- **Stratégie d'authentification du démarrage**

Pour les utilisateurs qui stockent des informations sensibles sur des appareils mobiles et ordinateurs portables, le chiffrement intégral du disque avec l'authentification avant le démarrage (par certificat) permet de s'assurer que les données se trouvant sur un appareil perdu ou volé ne seront pas exposées.

2. Les zones de sécurité et leur mécanisme de contrôle d'accès

- Le premier périmètre défense de système de sécurité basée sur le contrôle d'accès, est le contrôle des équipements réseau accédant au système grâce au réseau informatique. Il évalue l'identité et le groupe de sécurité des différents équipements réseau et la place dans leur instance (VLAN) respective. Il est chargé en aval d'alerter les tentatives d'instruction et de dissuader les pirates et les utilisateurs inconnus. Ce contrôle s'exécute sans aval de l'utilisateur, lors de la connexion sur le réseau.

- La deuxième ligne de défense de système de sécurité basée sur le contrôle d'accès, est la supervision de l'état des ordinateurs de service. Ce contrôle permet ou non l'accès à l'ensemble des services du système. L'évaluation s'effectue sur l'état de conformité des ordinateurs de service (le système Windows, présence du pare-feu activé, les mises à jour du système et de l'anti-virus et absence de vulnérabilité). Elle est chargée de gérer les connexions de l'ordinateur aux VLAN donnant accès aux services du système, une fois le contrôle d'autorisation réalisé. En aval, Elle est chargée d'alerter l'utilisateur des besoins de conformité du système de sécurité de la machine et de persuader les pirates et les utilisateurs inconnus.

- La troisième ligne de défense de système de sécurité basée sur le contrôle d'accès, est le contrôle de l'ouverture de session d'un utilisateur. Ce contrôle permet ou non l'accès à l'ensemble de services supportés en amont aux serveurs de service suivant le profil de l'utilisateur. Il veille à authentifier et à autoriser les utilisateurs accédant au système d'information lors de l'ouverture d'une session. Pour y parvenir nous avons adopté l'usage de mécanisme d'authentification fort qu'offre le contrôleur de domaine avec l'annuaire active directory. Ce contrôle est chargé de gérer l'ouverture d'une session de l'utilisateur suivant son profil dans le système, une fois le contrôle d'autorisation réalisé. En aval, il est chargé d'alerter les intrusions et à l'utilisateur ses besoins de conformité à la politique de sécurité et de persuader les pirates et les utilisateurs inconnus.

- La dernière ligne défensive de notre système de sécurité basée sur le contrôle d'accès, est constituée des contrôles des droits des utilisateurs sur les ressources du système d'information. Il délimite les droits qu'a un utilisateur lors de ces manipulations des ressources. Le contrôle s'effectuera sur les droits (permission) que possède un utilisateur sur une ressource donnée. Pour y arriver nous avons adopté l'usage d'un système de gestion des habilitations suivant, une politique de contrôle d'accès au sein de l'annuaire active directory.

V. Authentification sécurisée entre forêts par approbation

Lorsque deux forêts Windows Server sont connectées par une approbation de forêt, il est possible de router entre ces forêts des requêtes d'authentification exécutées au moyen du protocole Kerberos V5 ou NTLM, de manière à fournir l'accès aux ressources des deux forêts. Pour que les protocoles d'authentification puissent suivre le chemin d'approbation de la forêt, le nom du service principal (SPN, Service Principal Name) de l'ordinateur de la ressource est résolu dans un emplacement situé dans l'autre forêt. Un SPN peut être le nom DNS (Domain Name System) de l'hôte, le nom DNS du domaine où le nom unique de l'objet, point de connexion au service. Le protocole d'authentification utilisée est Kerberos, cela à ses diverses fonctionnalités, son efficacité et sa conformité à l'environnement technologique.

Lorsqu'une station de travail, dans une forêt, tente d'accéder à des données se trouvant sur l'ordinateur des ressources d'une autre forêt, Kerberos contacte le contrôleur de domaine pour qu'il lui procure un ticket de service pour le SPN de cet ordinateur. Après avoir interrogé le catalogue global et détecté que le SPN ne se trouvait pas dans la même forêt que lui, le contrôleur renvoie à la station de travail une référence à son domaine parent. La station demande alors le ticket de service au domaine parent, et suit la chaîne de références jusqu'au domaine où se trouve la ressource.

La figure suivante et les étapes correspondantes décrivent en détail le processus d'authentification Kerberos qui est mis en œuvre lorsque des ordinateurs tentent d'accéder aux ressources d'un ordinateur situé dans une autre forêt.

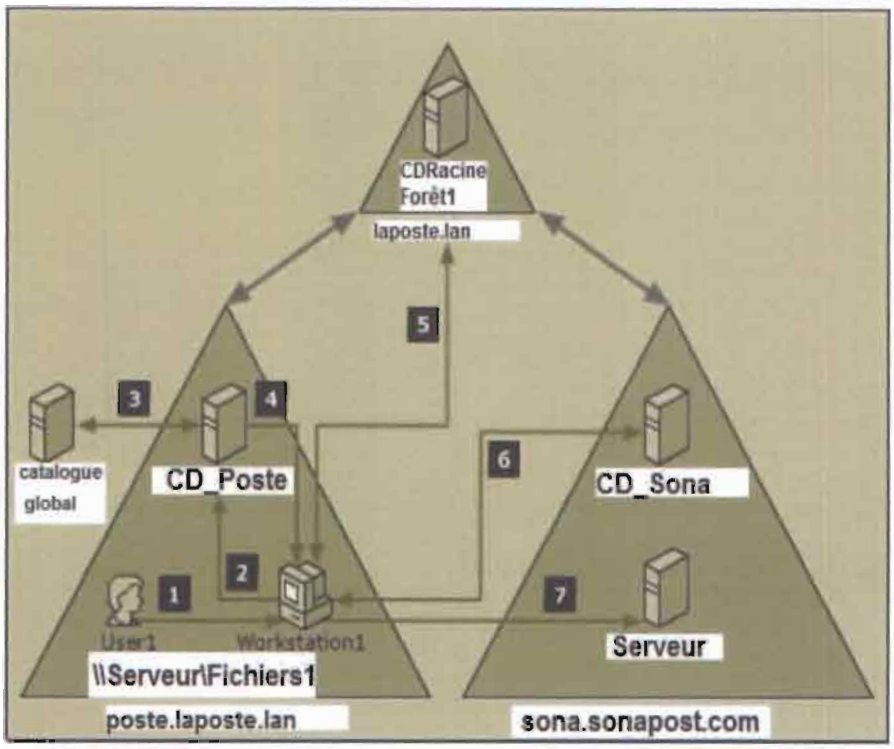


Figure 11 : Accès à des ressources

1. Utilisateur1 se connecte à Station1 en utilisant les informations d'identification fournies par le domaine **poste.laposte.lan**. L'utilisateur tente ensuite d'accéder à une ressource partagée sur **\\Serveur\Fichiers1** situé dans la forêt **sonapost.com**.
2. Station1 contacte le Centre de distribution de Clés (KDC, Key Distribution Center) sur un Contrôleur de Domaine de son domaine (**CD_Poste**) et demande un ticket de service pour le SPN de Serveur\Fichiers1.
3. **CD_ Poste** ne trouve pas le SPN dans sa base de données de domaines, et interroge donc le catalogue global afin de déterminer si ce nom existe dans l'un des domaines de la forêt microsoft.com. Un catalogue global étant limité à sa propre forêt, le SPN est introuvable. Le **catalogue global** recherche alors dans sa base de données des informations relatives à toute approbation établie avec sa forêt. Si sa recherche est fructueuse, il compare les suffixes de nom indiqués dans l'objet domaine d'approbation (TDO, Trusted Domain Object) de l'approbation avec le suffixe du SPN cible afin de trouver une correspondance. Dès qu'il en trouve une, il renvoie une indication de routage à **CD_Poste**.
4. **CD_Poste** renvoie à Station1 une référence à son domaine parent.

5. Station1 contacte un contrôleur de domaine de **CD_Racine_Forêt1** (son domaine parant) afin de lui demander une référence à un contrôleur de domaine (**CD_Racine_Forêt2**) se trouvant dans le domaine racine de la forêt msn.com.
6. Station1 contacte **CD_Racine_Forêt2**, dans la forêt msn.com, pour obtenir un ticket de service pour le service demandé.
7. **CD_Racine_Forêt2** contacte son catalogue global pour trouver le SPN. Le catalogue trouve une correspondance pour le SPN et la renvoie à **CD_Racine_Forêt2**.
8. **CD_Racine_Forêt2** renvoie alors à Station1 la référence à **sona.sonapost.com**.
9. Station1 contacte le KDC sur **CD_Sona** et négocie le ticket nécessaire à Utilisateur1 pour accéder à Serveur_Fichiers1.
10. Station1 envoie le ticket de service ainsi obtenu à Serveur_Fichiers1, qui lit les informations d'identification d'Utilisateur1 et crée un jeton d'accès à partir de ces informations.

Lors de la création d'une approbation de forêt, chaque forêt collecte tous les espaces de nom approuvés dans sa forêt partenaire et enregistre ces informations dans un TDO. Les espaces de nom approuvés sont les noms d'arborescence de domaine, les suffixes de nom d'utilisateur principal (UPN, User Principal Name), les suffixes de nom du service principal (SPN, Service Principal Name) et les espaces de nom ID de sécurité (SID, Security ID) utilisés dans l'autre forêt. Les objets TDO sont répliqués dans le catalogue global.

Les indications de routage ne sont utilisées que lorsqu'aucun des canaux d'authentification classiques (contrôleur de domaine local, puis catalogue global) n'a réussi à localiser un SPN. Ces indications aident à diriger les requêtes d'authentification vers la forêt de destination. Lorsqu'un SPN est introuvable dans le domaine d'où provient la requête d'ouverture de session sur le réseau et dans la base de données du catalogue global, ce dernier vérifie, dans le TDO d'approbation de la forêt, s'il existe des suffixes de nom approuvés situés dans l'autre forêt concordant avec le suffixe du SPN. S'il en trouve un, le domaine racine de la forêt renvoie une indication de routage à l'ordinateur source d'origine afin qu'il puisse poursuivre la localisation du SPN dans l'autre forêt.

REFERENCES

Bibliographie

Livres

- **CHAPITRE 3** :

- Jean François CARPENTIER.« LA SECURITE INFORMATIQUE DANS LA PETITE ENTREPRISE » EYROLLES.2008. 551 pages

- **CHAPITRE 4 :**

- WINDOWS 2008 SERVER CONFIGURATION ET DEPANNAGE D'UNE INFRASTRUCTURE RÉSEAU.ENI.2008.255 pages
- WINDOWS SERVE.2003.2008 . ENI.2008.455 pages
- Windows Serveur 2008 Administration avancée. ENI.2008.245 pages
- Windows Server 2008-Examen_MCTS_70-642.ENI.2008.987 pages
- Windows Server 2008 R2 INSTALLATION DEPANNAGE.ENI.2008.682 pages
- Windows server 2008 R2 Administration instant reference.ENI.2008.953 pages

Revues professionnelles, articles de presse et dossiers thematiques

- **CHAPITRE 1 :**

- CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS, Dossier technique « GESTION DES IDENTITES » du Juillet 2007

- **CHAPITRE 2, 3 ET 4** :

- Tom COEYTAUX et Gérard INEICHEN « LA TECHNOLOGIE DE CONTRÔLE D'ACCÈS RÉSEAU»HEG - Genève, 20.06.2012, 64 pages.

- Aziz Roger OUEDRAOGO et Kalifa OUEDRAOGO, « ETUDE POUR LE RENFORCEMENT DE LA SECURITE INFORMATIQUE AU SEIN DE LA SONAPOST. »2007,92 pages
- SUPINFO, « CONFIGURATION DU RBAC (ROLE-BASED ACCESS CONTROL) »
- SERGER BORDERES « AUTHENTIFICATION RESEAU AVEC RADIUS » 2006
- Elie MABO, « MODELE D'ARCHITECTURE D'IMPLEMENTATION D'UN CONTROLE D'ACCES TECHNIQUE A UN RESEAU D'ENTREPRISE » Janvier 2012
- Note du cours de l'université de Renne I, « AUTHENTIFICATION ET CONTROLE D'ACCES »2008.

Sites WEB

➢ **CHAPITRE 1 :**

www.univ-bobo.bf/(04/09/2013)

*www.**sonapost**.bf/*(04/09/2013)

➢ **CHAPITRE 3 :**

http://technet.microsoft.com/fr-fr/library/jj134043.aspx (04/09/2013 au 15/02/2014)

http://technet.microsoft.com/fr-fr/library/cc787646(04/09/2013 au 15/02/2014)

http://www.techno-science.net (16/09/2013)

http://www.wikipedia.org (02/09/2013 au 25/10/2013)

« Crains Dieu, et garde ses commandements; car c'est là le tout de l'homme. »