La technologie de contrôle d'accès réseau 802.1x et son implémentation pratique

Travail de diplôme réalisé en vue de l'obtention du diplôme HES

par :

Tom COEYTAUX

Conseiller au travail de diplôme :

Gérard INEICHEN

HEG - Genève, 20.06.2012

Haute École de Gestion de Genève (HEG-GE)

Filière Informatique de Gestion

Déclaration

Ce travail de diplôme est réalisé dans le cadre de l'examen final de la Haute école de gestion de Genève, en vue de l'obtention du titre de Bachelor en Informatique de Gestion. L'étudiant accepte, le cas échéant, la clause de confidentialité. L'utilisation des conclusions et recommandations formulées dans le travail de diplôme, sans préjuger de leur valeur, n'engage ni la responsabilité de l'auteur, ni celle du conseiller au travail de diplôme, du juré et de la HEG.

« J'atteste avoir réalisé seul le présent travail, sans avoir utilisé des sources autres que celles citées dans la bibliographie. »

Fait à Genève, le 25.01.2012

Tom Coeytaux

Remerciements

Je tiens tout d'abord à remercier Monsieur Gérard Ineichen qui a accepté de me soutenir et de me guider dans l'élaboration de ce travail de diplôme. Il m'a également fourni gracieusement tout l'équipement nécessaire à sa réalisation, que ce soit le lieu de travail ou l'infrastructure technique. Ces conseils et remarques m'ont aussi permis d'aiguiller ma recherche. Pour tout cela, un grand merci.

Je remercie aussi mon père pour sa relecture attentive et ses suggestions de lecture.

Résumé

La sécurité informatique est un enjeu qui gagne en importance au fil du temps. Les attaques et intrusions sont relatées dans la presse (électronique et papier) tellement souvent que cela en devient banal. Les attaques de vers et virus informatiques se répandant sur les réseaux des entreprises et écoles est une problématique toujours d'actualité. Bref, la sécurité informatique n'a jamais été un investissement aussi indispensable qu'aujourd'hui. En effet, de nouvelles menaces font leur apparition chaque jour et les risques qui en découlent peuvent entraver gravement les opérations du système informatique et par conséquent, le business continuity[1].

Parmi ces menaces, celle des employés. Souvent sous-estimée, celle-ci est pourtant non négligeable. Selon un rapport de la centrale d'enregistrement et d'analyse pour la sureté de l'information de la confédération datant de 2011 : « 85,7 % des sociétés suisses permettent à leur personnel de raccorder à leur réseau Intranet un périphérique externe […]. Dans 86,7 % des cas, les employés peuvent prendre à la maison l'ordinateur du bureau et donc le raccorder à des réseaux tiers. »[2]. Il suffit donc qu'un membre du personnel se branche au réseau d'entreprise en faisant fi des impératifs de sécurisation de sa machine et c'est l'entreprise toute entière qui court alors un risque. On ne veut alors pas seulement savoir qui accède au réseau, mais où, quand et comment cela a eu lieu. Idéalement, on veut savoir si l'on peut faire confiance au périphérique qui se connecte. On protège souvent efficacement un réseau sans-fil d'entreprise, en limitant l'accès au strict minimum (Internet en général) car celui-ci peut être atteint plus facilement par les menaces externes, mais le réseau câblé ne doit pas être mis de côté pour autant.

C'est dans ce contexte que mon travail de diplôme s'inscrit, réfléchissant à une solution appropriée afin non pas d'interdire l'accès au réseau câblé pour les machines externes à l'entreprise, mais pour en sécuriser l'accès et réduire les risques de subir un préjudice ce faisant. La solution doit permettre d'avoir un contrôle centralisé et efficace sur les accès. Ce travail s'articule autour de l'utilisation du réseau par rapport à des restrictions de lieu, d'identité et d'heures d'accès. Il développe cependant principalement l'aspect de la sécurisation par vérification de l'état de santé du client demandant l'accès aux ressources d'entreprise.

---

[1] Business continuity : continuité des opérations rapportant de l'argent à l'entreprise

[2] Rapport MELANI 2011/1

Table des matières

Liste des figures

Introduction

L'idée de ce travail a germé au cours de mes lectures sur le site web Technet[3]. Je cherchais de la documentation à propos de Windows Server 2008. De fil en aiguille, j'ai appris que ce système d'exploitation pouvait être utilisé comme contrôleur d'accès pour des clients Windows en vérifiant l'état de leur protection et le statut des mises à jour système. J'ai aussi eu l'occasion lors des cours ici à la HEG de pouvoir implémenter et tester l'authentification des équipements réseaux grâce à un serveur, ce qui une prémisse à la mise en œuvre de la méthode de contrôle d'accès réseau par port. Pour pouvoir mettre en œuvre une sécurité du réseau d'entreprise contre ses employés, j'ai décidé de faire un laboratoire de test afin d'élaborer des directives à la mise en place de ce contrôle. Les deux grands acteurs du marché informatique dont les produits sont testés dans ce travail proposent un ou plusieurs outils permettant ce contrôle des accès.

Chez Cisco[4], l'outil testé fait partie d'une suite de périphériques et de logiciels qui porte le nom de « Self-Defending Network », car le réseau totalement équipé doit être en mesure de prévenir et/ou de contenir les attaques que peut subir l'infrastructure. Le produit testé est celui qui est au centre du contrôle des accès, celui-ci ne propose pas de vérification d'état de santé du client. C'est le « Secure Access Control Server ».

Chez Microsoft, les fonctionnalités utilisées font partie des rôles et fonctionnalités que propose Windows Server 2008. Les fonctions désirées doivent être installées avant de pouvoir être utilisées. Le contrôle d'accès réseau sur ce produit permet de vérifier l'état de santé du client et c'est ce point qui sera développé en laboratoire, car c'est un point de sécurité important à implémenter pour assurer la sécurité d'un réseau.

Pour faire fonctionner le tout, le protocole mis en œuvre et dont le fonctionnement va être détaillé se nomme 802.1X. Celui-ci est indispensable à la bonne communication entre les périphériques chargés de l'authentification et à la distribution d'autorisations pour les clients.

Pour des raisons qui incombent à la réalité du métier, beaucoup de termes techniques anglais ne sont pas traduits afin ne pas surcharger le document inutilement.

---

[3] Ressources techniques informatiques de Microsoft

[4] Cisco Systems, Inc.

1. Contexte

1.1 La technologie 802.1x

1.1.1 De quoi parle-t-on ?

802.1X est un standard qui a été créé dans le but de sécuriser les réseaux locaux filaires ou sans-fil. Il a été mis au point par l'IEEE[5] en 2001. Il est mis à jour régulièrement, d'ailleurs sa dernière révision date de 2010. Si l'ont traduit sa définition de l'anglais, 802.1x est un contrôle d'accès réseau basé sur le port. L'objectif de 802.1X est de délivrer, ou non, un droit d'accès au réseau, ceci sans se soucier du support physique utilisé. En effet, 802.1X travaille au niveau de la couche 2 du modèle OSI[6] et ne requiert pas l'utilisation de la couche 3 (couche IP). En général, l'accord du droit d'accès permet ensuite d'utiliser le protocole Ethernet[7] et de permettre également l'accès à divers mécanismes d'auto-configuration, que ce soit un démarrage depuis le réseau ou une configuration IP attribuée automatiquement.

Trois éléments indispensables doivent être présents pour permettre le bon fonctionnement de ce processus :

- Un client réseau/une machine que nous appellerons système à authentifier[8].
- Le système authentificateur, qui va s'occuper de transmettre la demande d'autorisation à l'élément suivant.
- Le serveur d'authentification. Celui-ci applique les règles d'accès définies nécessaires à une décision d'autorisation puis renvoie une réponse (acceptation ou rejet).

Le système authentificateur surveille l'état d'un support physique dans l'attente d'un client à authentifier qui souhaite disposer des ressources associées à ce même support. Une fois la demande reçue, il fait le relais avec le serveur d'authentification sans s'immiscer dans le dialogue client/serveur, il ne fait qu'attendre la décision du serveur qui lui est destinée.

---

[5] IEEE : L'Institute of Electrical and Electronics Engineers est un organisme chargé de définir des normes dans le monde des télécommunications, mais aussi dans le domaine informatique et électrique.

[6] OSI : Open Systems Interconnection – Voir annexe 2 : Modèle OSI

[7] Pour une définition d'Ethernet, voir annexe 1 : Glossaire

[8] "supplicant" en anglais

En plus d'un accès refusé ou accepté au port Ethernet, ce standard permet aussi l'attribution d'autorisations supplémentaires en cas d'accès accordé. Par exemple, une attribution de sous-réseau. Ces autorisations supplémentaires sont fournies par le serveur d'authentification et seront vues plus en détails dans la suite de ce travail.

1.1.2 Comment cela fonctionne-t-il ?

En pratique, le contrôle d'accès 802.1X fonctionne sur un port physique qui autorise ou non l'accès au niveau de la couche 2 (du modèle OSI) à un périphérique branché sur ce port. Mais lorsque l'accès n'est pas encore accordé, le système à authentifier et l'authentificateur doivent tout de même communiquer ensemble. Comment est-ce possible ? Concrètement, le port physique est divisé en deux ports virtuels dont un sera dédié à l'accès réseau standard, tel que le port physique l'assure normalement. Ce port est contrôlé, il peut être « fermé » ou « ouvert » à la communication. Le deuxième port virtuel se dédie uniquement aux trames 802.1x et il garantit donc la communication avec le serveur d'authentification. Ce modèle est valable qu'importe le support physique (fibre, wifi, câble).

802.1X encapsule par-dessus d'autres mécanismes d'authentification qui existaient déjà avant son apparition. Les messages 802.1X sont donc transportés par le biais de trames Ethernet EAPOL[9] qui sont seules autorisées à transiter sur un port en mode fermé. Dans ces trames se trouvent des échanges EAP, celles-ci seront ré-encapsulées depuis le système authentificateur (sans modification) dans un format que le serveur d'authentification peut comprendre (RADIUS[10] ou TACACS+[11]).

Le schéma sur le début de la page suivante illustre les messages échangés entre les 3 parties qui prennent part au mécanisme d'authentification, en montrant également l'utilisation d'attributs RADIUS attribuant un VLAN[12] au client, tel que démontré dans la suite de ce travail. C'est le système authentificateur (le switch) qui place le client dans le VLAN précisé par le serveur d'authentification. C'est le seul message qui est important pour lui, le reste de la communication se déroule uniquement entre le client et le serveur d'authentification et le switch ne sert qu'à relayer et à dé-encapsuler/ré-encapsuler les messages jusqu'à la décision du serveur.

---

[9] EAP Over Lan. Voir chapitre sur EAP.

[10] Remote Authentication Dial-In User Service – Voir annexe 1 : Glossaire

[11] Terminal Access Controller Access-Control System – Voir annexe 1 : Glossaire

[12] Virtual LAN : Réseau local virtuel

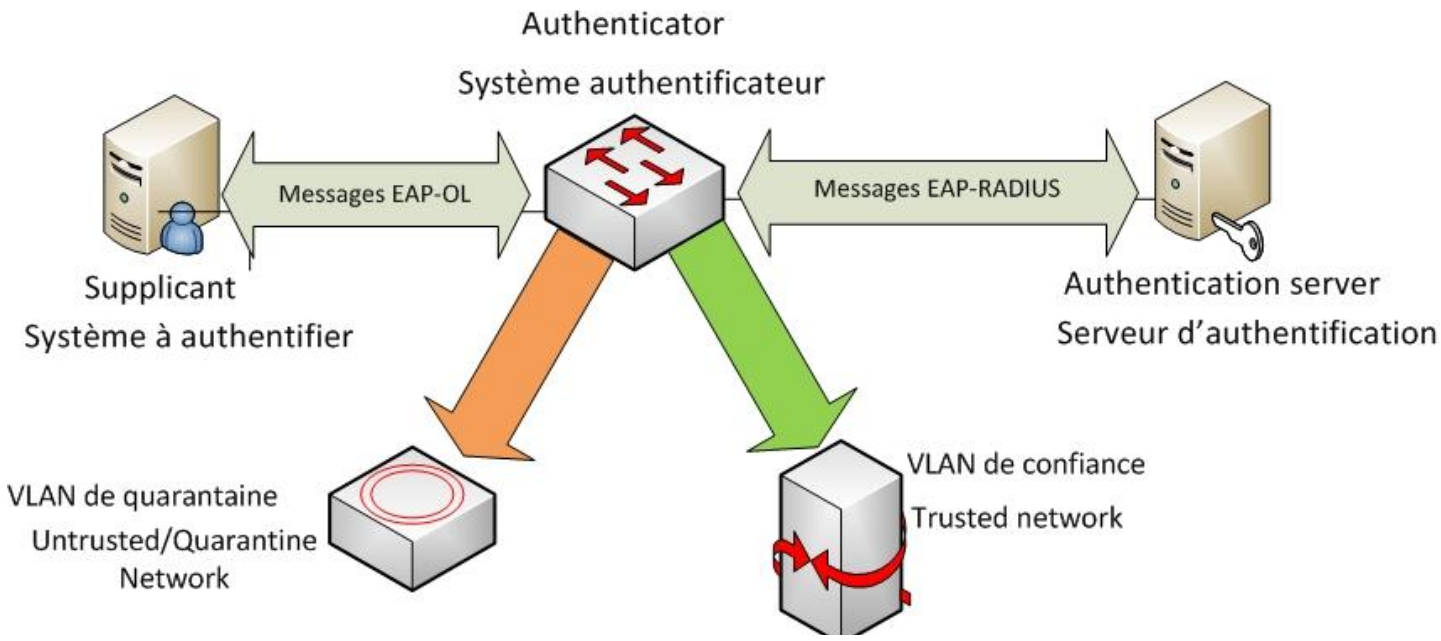

Figure 1: schéma 802.1X

1.1.2.1 EAP et ses déclinaisons

Extensible Authentication Protocol a été prévu à l'origine pour fournir une authentification (extensible) pour PPP[13]. Il ne nécessite pas de couche IP pour fonctionner. Il a ensuite été utilisé pour 802.1X, IKEv2[14] et les réseaux sans-fil. EAP étant comme son nom l'indique extensible, nous allons rapidement parler de ses déclinaisons.

1.1.2.1.1 LEAP

LEAP signifie « Light Extensible Authentication Protocol », qui se traduit par : version allégée de EAP. C'est une implémentation propriétaire d'EAP développée par Cisco. Lorsque que les mots de passes utilisés sont complexes, il est également très sûr. Ce qui a été mis en doute en cas d'utilisation d'un mot de passe faible. On préfèrera donc à sa place PEAP, EAP-TLS ou EAP-FAST pour l'aspect plus sécurisé de ces implémentations. LEAP n'est d'ailleurs pas supporté sur Windows sans l'ajout d'un client spécifique. Il est cependant largement supporté sur les points d'accès Wifi.

1.1.2.1.2 PEAP

PEAP signifie « Protected Extensible Authentication Protocol ». PEAP est une des implémentations d'EAP les plus utilisées. Elle utilise le protocole CHAP[15] pour authentifier de façon sécurisée un client grâce au challenge request/response. Windows Server utilise cette version d'EAP et elle est utilisée dans ce laboratoire.

---

[13] Point-to-Point Protocol

[14] Internet Key Exchange Protocol version 2

[15] Challenge-Handshake Authentication Protocol

1.1.2.1.3 EAP-TLS

EAP-TLS utilise un système d'authentification avec certificats. C'est donc l'un des meilleurs en termes de sécurité. Son désavantage réside dans le fait qu'un certificat doit être obligatoirement installé chez le client.

1.1.2.1.4 EAP-TTLS

EAP-TTLS fonctionne sur le même principe que la version ci-dessus, à la différence que le client ne nécessite pas de certificat de son côté. Un tunnel encrypté est créé à l'aide du certificat du serveur afin d'échanger les informations d'authentification.

1.1.2.1.5 EAP-FAST

FAST veut dire « Flexible Authentication via Secure Tunneling ». C'est une version améliorée de LEAP qui utilise PAC (Protected Access Credential), un set d'informations d'authentification qui ne peut pas être copié d'une machine à une autre. Il corrige le manque de sécurité qu'on attribue souvent à LEAP.

1.1.3 Compatibilité

La compatibilité du protocole 802.1x sur les systèmes d'exploitation des clients est assurée sur Windows depuis le service pack 3 de XP.

Sur Mac, le protocole est utilisable depuis la version 10.3 de Mac OS X.

Pour Linux, l'installation de modules complémentaires tels que « xsupplicant » est nécessaire pour permettre le fonctionnement de ce type d'authentification. A ma connaissance ce n'est pas supporté en natif.

1.1.3.1 Périphérique non 802.1X

Beaucoup de périphériques aujourd'hui n'intègrent pas le protocole 802.1x. C'est le cas par exemple d'une majorité d'imprimantes, mais également de projecteurs qui peuvent être connectés et contrôlés via le réseau d'entreprise. La solution de sécurité alternative dans ce cas-là, consiste à appliquer une règle de sécurité au port auquel est connecté le périphérique en question. Cette règle ne doit autoriser qu'une seule adresse physique, celle du périphérique en question. Si ce même périphérique dispose d'un accès sans-fil, l'idéal (à mon avis) serait de la connecter par le biais d'un SSID[16] caché muni d'un chiffrement WPA2 (réputé impénétrable dans la pratique, du fait du

[16] Service Set Identifier

changement constant des clés de chiffrement). Une variante consisterait à utiliser le 802.1X sans-fil en lieu et place du 802.1x filaire qui n'est pas présent sur le périphérique. Une solution sérieuse, en complément de la restriction d'une adresse physique sur le port, est celle qui est implémentée ici à la Haute Ecole. Le principe est d'affecter aux ports imprimantes par exemple, un VLAN différent. Ce VLAN n'est pas amené à changer et toutes les imprimantes se trouvent sur celui-ci. Le serveur d'impression a lui aussi accès à ce réseau séparé, tout en ayant accès au réseau principal. Le maillon faible peut se trouver ensuite sur ce serveur, mais l'accès direct aux ressources internes est totalement impossible dans cette configuration. C'est donc une bonne architecture à mettre en place.

2. Laboratoire

2.1 Matériel utilisé

2.1.1 Périphériques réseaux

2.1.1.1 Routeur

Le routeur de notre laboratoire, que nous nommerons « RLAB » sert à diriger le trafic du réseau du labo vers le réseau de l'école et vice versa. Il effectue une transformation des adresses internes du réseau du labo vers une seule adresse unique extérieure qui donne sur le réseau de l'école. Cette méthode est appelée PAT (Port Address Translation). Voici les caractéristiques techniques du routeur pour commencer.

Marque	Modèle	Système d'exploitation	Interfaces
Cisco	2621	IOS 12.2	1xEthernet, 2xFa, 2xSerial, 1xISDN

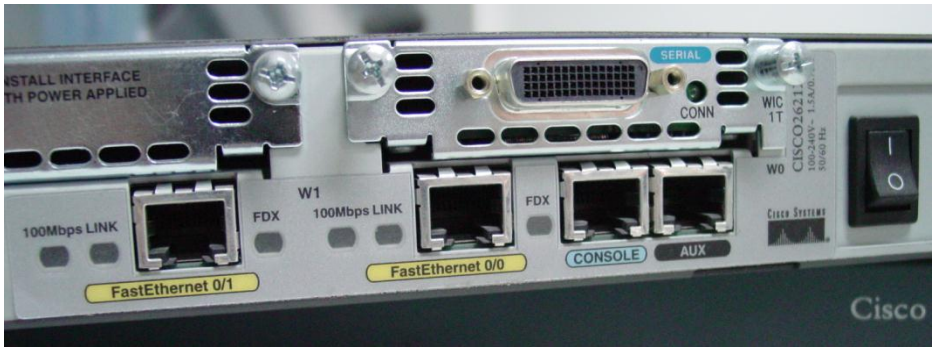

Figure 2: Routeur Cisco 2621, Source: http://xuyuanchao.ie.cnu.edu.cn

2.1.1.2 Switch

Le switch, ou commutateur, est un élément central de notre système d'authentification. C'est lui qui va appliquer les autorisations qu'il reçoit d'un des serveurs d'authentification en déplaçant le client sur le VLAN (sous-réseau virtuel) approprié. Les caractéristiques des switchs que j'ai pu tester durant mon expérimentation sont décrites ci-dessous. Le deuxième permet d'agir au niveau de la couche 3 du modèle ISO mais ne provoque aucun changement dans le fonctionnement du laboratoire.

Marque	Modèle	Système d'exploitation	Interfaces	Autre
Cisco	Catalyst 2950	IOS 12.1	24xFa,2xGi	L2 seulement
Cisco	Catalyst 3550	IOS 12.1	24xFa,2xGBIC	L2 & L3

Figure 3: Switch Cisco Catalyst 2950C, Source: http://media.ldlc.com

Figure 4: Switch Cisco Catalyst 3550, Source: http://www.powersourceonline.com

2.1.2 Ordinateurs/PC

J'ai à ma disposition pour mon étude trois stations de travail fonctionnant toutes sur Windows 7. Pour mes tests, je n'ai eu besoin que d'une seule machine client. Voici une description sommaire de ce matériel.

Marque	Modèle	Système d'exploitation	Interface
Dell	Optiplex 745	Windows 7 Pro 64 bits	1xGigabitEthernet

2.1.3 Serveurs et machines virtuelles

Il a été mis généreusement à ma disposition sur un des serveurs de virtualisation de la HEG un espace disque et des ressources pour créer les machines virtuelles nécessaires à ce laboratoire. Tout le détail sur ces machines est donné dans la section suivante concernant la topologie du laboratoire.

2.2 Topologie du labo

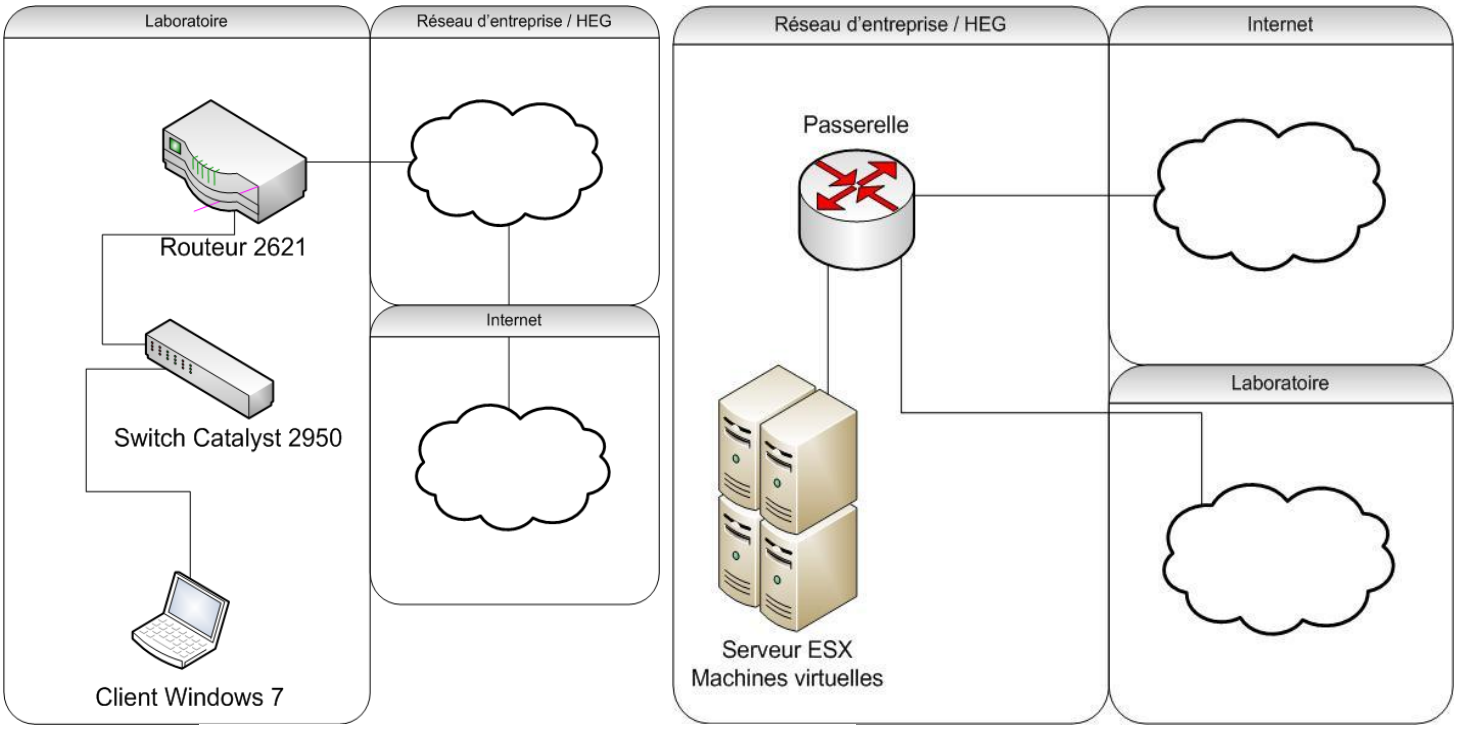

Figure 5: Schéma du laboratoire

2.2.1 Partie laboratoire

2.2.1.1 Routeur 2621

Le routeur du labo, nommé « RLAB » possède deux IP. Une sur le réseau HEG, l'autre sur le réseau du laboratoire. Ses IP sont respectivement 10.136.3.254 (masque 255.255.252.0) et 192.168.1.1 (masque par défaut).

2.2.1.2 Switch 2950/3550

Le switch possède l'IP 192.168.1.2 (masque par défaut) sur le réseau du laboratoire.

2.2.1.3 Client Windows 7

Le client se connectant au réseau d'entreprise reçoit une IP du routeur correspondant au VLAN sur lequel il est placé. Cela est expliqué plus en détails par la suite. La connexion du client au switch est contrôlée par le système d'authentification 802.1X.

2.2.2 Partie Réseau d'entreprise / HEG

Cette partie du réseau est la partie à protéger d'un accès non autorisé. Elle permet d'accéder non seulement à Internet par son biais, mais aussi à toutes les ressources internes de l'entreprise (les serveurs par exemple).

2.2.2.1 Passerelle

Dans ce cas précis, notre passerelle vers Internet et vers nos machines virtuelles possède l'IP 10.136.0.21. C'est un routeur du réseau HEG (sur le VLAN 9) qui sait où diriger les paquets pour fournir un accès à Internet ou à un autre réseau.

2.2.2.2 Serveur ESX et machines virtuelles

Le laboratoire fait usage de trois machines virtuelles hébergées sur le serveur ESX de la HEG. Deux machines virtuelles Windows Server 2008 R2 en font partie et se nomment respectivement DC1 et NPS[17]. Un contrôleur de domaine et un contrôleur d'accès réseau. Ceux-ci travaillent en tandem. Il faut cependant noter que l'utilisation d'un seul serveur pour ces deux rôles est également possible. Cela réduit cependant la stabilité et augmente le niveau de complexité du système en ne séparant pas clairement les responsabilités. Il y a ensuite une machine virtuelle embarquant le

[17] Network Policy Server

système Cisco Secure Access Control System, plus communément appelé ACS, qui par ailleurs est également le nom donné à la VM.

2.2.2.2.1 DC1

Ce serveur possède l'IP 10.136.3.250 avec un masque de sous-réseau de 255.255.252.0. Il se trouve sur le VLAN 9 du réseau de la HEG.

Il agit comme contrôleur du domaine « bachelor.ch » qui est le domaine Active Directory de test de ce laboratoire d'expérimentation.

2.2.2.2.2 NPS

Ce serveur possède l'IP 10.136.3.251 avec le même masque de sous-réseau que précédemment : 255.255.252.0

Il agit comme contrôleur d'accès réseau, il est contacté par l'authentificateur (Switch) pour communiquer puis attribuer des autorisations à un périphérique souhaitant s'authentifier.

2.2.2.2.3 Cisco Secure Access Control (ACS)

Ce serveur a l'IP 10.136.3.252 / 255.255.252.0

Il est localisé physiquement au même endroit que les autres machines virtuelles, sur le Serveur ESX dans notre schéma. Une interface graphique accessible depuis un navigateur est utilisée pour la configuration du système d'authentification.

2.2.3 Partie Internet

Une fois que le client a un accès réseau autorisé, l'accès à Internet peut se faire depuis le client uniquement si celui-ci définit le proxy HES dans son navigateur (proxyhes.etat-ge.ch). Autrement l'accès à Internet n'est pas possible (A quelques exceptions près).

2.3 Configuration

2.3.1 Configuration du routeur

Le routeur va s'occuper de distribuer des adresses IP aux clients. Il a aussi la tâche de séparer les clients en quarantaine des clients autorisés et de leur fournir un accès totalement différent au réseau. Plus de détails avec la configuration du routeur de ce laboratoire ci-dessous.

2.3.1.1 Interfaces

L'interface reliée au réseau extérieur, le réseau de l'école, est l'interface FastEthernet 0/0. Nous lui attribuons l'adresse IP 10.136.3.254, qui est et sera la seule et unique adresse visible de notre laboratoire sur le réseau externe.

```
# Interface FastEthernet 0/0
# ip address 10.136.3.254 255.255.252.0
# ip nat outside
# no shutdown
```

La commande "ip nat outside" a toute son importance, car elle permet de spécifier que c'est cette interface qui va être utilisée pour comme lien extérieur pour la transformation d'adresses internes. Cela va être expliqué par la suite. L'activation du lien se fait par la commande de désactivation du mode éteint de celui-ci, c'est la commande « no shutdown » qui accomplit cette action.

La prochaine interface à configurer est celle du côté de notre laboratoire. C'est un peu plus complexe car elle répond de plusieurs sous-réseaux virtuels sur une seule patte physique. Pour créer des interfaces virtuelles, nous allons utiliser les sous-interfaces.

```
# Interface FastEthernet 0/1.1
# Encapsulation dot1Q 1 native
# ip address 192.168.1.1 255.255.255.0
# ip nat inside
```

La première sous-interface agit comme passerelle du VLAN 1. Le VLAN de gestion des équipements. Chaque équipement (en l'occurrence le routeur et le switch) possède une IP statique qui permet sa gestion sur ce VLAN. Une encapsulation est nécessaire pour pouvoir tagger les paquets avec le numéro du VLAN concerné. Ceci se fait en précisant le format 802.1q (dot1q) qui est le standard utilisé pour cette opération. Nous précisons également que le VLAN 1 est le VLAN natif, il n'est donc par défaut pas tagué. Ceci peut être dangereux car cela nous rend vulnérable à l'attaque dite du paquet doublement tagué. Pour tout de même donner un tag au VLAN natif, il faut

activer la commande globale « vlan dot1q tag native ». Ce qui a pour effet de sécuriser notre environnement. Ici aussi la commande « ip nat inside » est indispensable pour préciser que cette interface possède une IP qui doit être transformée avant d'accéder au réseau externe au laboratoire.

```
#  interface FastEthernet0/1.2
#   encapsulation dot1Q 2
#   ip address 192.168.2.1 255.255.255.0
#   ip access-group allowonlyNPS in
#   ip nat inside
```

Cette deuxième sous-interface sera la passerelle du VLAN restrictif, le numéro 2. Les commandes sont les même que pour la première, mais nous ajoutons la commande « ip access-group allowonlyNPS » qui permet d'appliquer une liste de contrôle d'accès. Celle-ci va être explicitée plus loin, mais son nom devrait à lui seul expliquer son utilité.

```
#  interface FastEthernet0/1.3
#   encapsulation dot1Q 3
#   ip address 192.168.3.1 255.255.255.0
#   ip access-group deny3to24 in
#   ip nat inside
```

Ici aussi, pour notre VLAN 3 autorisé nous définissons l'encapsulation des paquets avec le tag correspondant ainsi qu'une liste de contrôle d'accès à appliquer à ce sous-réseau. La commande NAT est également présente pour dire au routeur de transformer ce réseau d'IP avant sa sortie sur le réseau extérieur.

```
#  interface FastEthernet0/1.4
#   encapsulation dot1Q 4
#   ip address 192.168.4.1 255.255.255.0
#   ip access-group deny4to23 in
#   ip nat inside
```

La configuration est identique pour notre VLAN de réserve.

2.3.1.2 Routage des paquets

Pour pouvoir communiquer avec le réseau de l'école qui est en place, il est nécessaire de donner aux paquets une route à suivre. Ceci va se faire sur le routeur et permettre de connaître la route à utiliser pour acheminer correctement un paquet d'une source A jusqu'à sa destination B. Dans notre cas, nous ne voulons pas informer les autres routeurs du réseau des réseaux que nous possédons, car nous n'attendons aucun paquet en entrée, sauf ceux qu'y répondent à une demande que nous avons-nous même envoyée au préalable. Pour envoyer nos paquets vers l'extérieur, une seule commande suffit, nous allons créer une route par défaut statique.

```
#  ip route 0.0.0.0 0.0.0.0 10.136.0.21
```

Que va faire exactement cette commande ? Elle spécifie simplement que les paquets ayant n'importe quelle destination seront envoyés vers la passerelle par défaut 10.136.0.21 pour que celle-ci les dirige au bon endroit.

Nous pouvons vérifier que la route est prise en compte en tapant :

```
#  show ip route
```

2.3.1.3 Service DHCP

```
#  ip dhcp excluded-address 192.168.2.20 192.168.2.255
#  ip dhcp excluded-address 192.168.3.20 192.168.3.255
#  ip dhcp excluded-address 192.168.4.20 192.168.4.255
#  ip dhcp excluded-address 192.168.2.1 192.168.2.9
#  ip dhcp excluded-address 192.168.4.1 192.168.4.9
#  ip dhcp excluded-address 192.168.3.1 192.168.3.9
```

Nous précisons les adresses IP qui ne doivent pas être attribuées par le service DHCP. Le VLAN de gestion en 192.168.1.0 possède uniquement des équipements ayant une adresse IP statique. Il n'y a donc pas de service DHCP pour ce sous-réseau. Pour les autres sous-réseaux (VLAN 2, 3,4) les attributions d'IP sont automatisées et l'on attribue les IP entre .10 et .19 ce qui permet de maitriser parfaitement l'attribution des adresses dans ce contexte de labo. Nous configurons ensuite les « pools » DHCP pour chaque VLAN. Pour l'instant le VLAN 4 est un VLAN de réserve pour un éventuel usage ultérieur.

```
#  ip dhcp pool vlan2
#  network 192.168.2.0 255.255.255.0
#  default-router 192.168.2.1
#  domain-name bachelor.ch
#  netbios-name-server 160.53.236.30
#  dns-server 160.53.236.30
```

Les commandes pour le pool des autres VLAN 3 et 4 sont identiques à l'exception du sous-réseau qui est différent. Nous précisons la passerelle par défaut à utiliser pour le client, ainsi que les serveurs de résolutions de noms, indispensables à la navigation sur Internet notamment.

2.3.1.4 Service NAT

Le service de « Network Address Translation » s'occupe de transformer un jeu d'adresse IP entre deux réseaux dont l'adressage est incompatible afin que ceux-ci puissent communiquer. En général le NAT transforme une adresse en une autre. C'est le « one-to-one », mais dans notre cas, nous surchargeons une seule IP externe avec

plusieurs IP internes. La commande « overload » permet de le préciser. Ce mode de NAT est aussi appelé PAT, pour « Port Address Translation ». Plutôt que d'utiliser plusieurs IP, on utilise plusieurs numéros de port sur la même IP, ce qui permet de retrouver à quel canal de communication appartient quelle information.

```
#  ip nat inside source list 1 interface FastEthernet0/0 overload
#  access-list 1 permit 192.168.1.1
#  access-list 1 permit 192.168.1.2
#  access-list 1 permit 192.168.3.0 0.0.0.255
#  access-list 1 permit 192.168.2.0 0.0.0.255
```

Dans la première commande, nous précisons aussi la liste d'adresses à transformer. Nous faisons d'abord référence au numéro de la liste où ces IP sont listées. Nous créons ensuite la liste ligne par ligne, une pour chaque IP, chaque réseau ou sous-réseau. Dans ce laboratoire, je permets le NAT sur les adresses statiques du matériel dans le VLAN de gestion, ainsi que le VLAN 2 (restrictif) et le VLAN 3 (autorisé). Pourquoi le VLAN 2 ? Bonne question, la réponse est dans la section suivante.

2.3.1.5 ACL

Les ACL (Listes de contrôle d'accès) vont nous permettre de définir des règles d'accès précis pour chaque VLAN séparément. Rappelez-vous, nous avons défini que la sous-interface 2 utilise la règle d'accès « allowonlyNPS ». Voici maintenant sa définition.

```
#  ip access-list extended allowonlyNPS
#   permit tcp 192.168.2.0 0.0.0.255 host 10.136.3.251 eq www
#   deny   ip any any
```

Comme vous le constatez, cette liste permet l'accès à tout le sous-réseau du VLAN 2 au serveur de remédiation, lors du labo Windows Server 2008. De plus, seul le protocole http est autorisé, car c'est le seul utile à la récupération du logiciel antivirus. Cela évite de s'exposer à des attaques sur d'autres ports. Ce sous-réseau n'a par contre accès à aucun autre emplacement que celui-ci. Bien que les adresses de ce sous-réseau aient été configurées pour être transformées vers l'extérieur, il n'en sera rien à moins que la destination corresponde au serveur de remédiation. Moyen très efficace de restreindre l'accès du VLAN restrictif. Nous configurons ensuite la liste de contrôle d'accès pour la troisième sous-interface, celle qui est attribuée au VLAN 3 (qui est le VLAN autorisé).

```
#  ip access-list extended deny3to24
#   deny   ip 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255
#   deny   ip 192.168.3.0 0.0.0.255 192.168.4.0 0.0.0.255
#   permit ip any any
```

Cette liste d'accès permet de restreindre l'accès aux autres VLAN. En effet, aucun VLAN n'est sensé communiqué avec un autre dans notre configuration. Cela casserait toute la logique de notre implémentation. La liste d'accès suivante est celle du VLAN 4. Elle est quasiment identique à la précédente. Le principe est totalement le même.

```
# ip access-list extended deny4to23
# deny   ip 192.168.4.0 0.0.0.255 192.168.2.0 0.0.0.255
# deny   ip 192.168.4.0 0.0.0.255 192.168.3.0 0.0.0.255
# permit ip any any
```

2.3.2 Configuration du switch

Le switch agit comme transporteur d'informations d'authentification jusqu'au serveur, il attend ensuite sa réponse pour savoir comment agir et quelles autorisations donner au client demandant l'accès.

Pour la configuration, je vais énumérer les commandes importantes et expliquer leur utilité dans le contexte de notre labo. Pour des raisons évidentes de sécurité, l'encryption des mots de passe est activée et l'on utilise le « enable secret » pour hacher le mot de passe administrateur.

2.3.2.1 Service AAA

La première étape consiste à configurer le service d'authentification, autorisation et accounting (AAA). Ceci se fait avec les commandes suivantes :

```
# aaa new-model
# aaa authentication dot1x default group radius
# aaa authorization network default group radius
# radius-server host 10.136.3.25x auth-port 1812 acct-port 1813 key 7 s3cr3t
```

Le "aaa new-model" active avec effet immédiat l'authentification locale sur toutes les interfaces et lignes vty. La ligne console reste cependant accessible normalement.

Les deux commandes suivantes définissent le groupe de serveurs à utiliser pour authentifier et attribuer des autorisations aux utilisateurs. En l'occurrence ici, notre groupe de serveurs RADIUS, qui n'est en fait qu'un seul serveur dans notre cas. On donne ensuite l'adresse de notre serveur RADIUS, les ports qu'il utilise pour communiquer ainsi que le mot de passe.

2.3.2.2 Service 802.1X

Une fois les références données, la prochaine étape consiste à activer le contrôle des ports pour l'authentification 802.1x. Ceci se fait avec la ligne suivante :

```
# dot1x system-auth-control
```

2.3.2.3 Interfaces

Nous passons l'interface reliée au routeur en mode trunk[18], afin qu'elle n'ait pas besoin d'authentification et qu'elle puisse supporter plusieurs VLAN différents.

```
# interface FastEthernet0/1
# switchport trunk encapsulation dot1q
# switchport mode trunk
```

Les ports numéro 10 et 11 du switch sont deux ports controlés par 802.1x. Voici la configuration correspondante.

```
# interface range FastEthernet 0/10-11
# switchport mode access
# dot1x port-control auto
```

On spécifie en premier que le port n'aura le droit qu'à l'accès à un VLAN unique et qu'il n'y a pas d'agrégation de VLANs sur ce lien. On configure ensuite le port-control en auto, ce qui a pour effet d'activer le contrôle du port par 802.1x.

Avec ce contrôle de port, une seule machine pourra être authentifiée en tout temps. En effet, même avec un hub ou des machines virtuelles, l'accès ne sera accordé qu'à une seule machine, qu'elle soit physique ou virtuelle. Sur les Switchs Catalyst 4500 et 6500, il est possible de permettre l'authentification de multiples équipements sur un seul port de switch, que ce soit des machines virtuelles ou des machines physiques branchées sur un Hub. C'est n'est pas le cas sur nos Catalyst 2950 et 3550.

```
# interface FastEthernet0/12
# switchport access vlan 3
# switchport mode access
```

Le port 12 pourrait être utilisé pour simuler un serveur d'entreprise contenant des fichiers accessibles uniquement aux clients autorisés. Il se trouverait donc sur le VLAN 3, qui est le VLAN autorisé. Il ne serait pas accessible aux clients en quarantaine sur le VLAN 2.

```
# interface Vlan1
# ip address 192.168.1.2 255.255.255.0
```

Bien sûr, il faut attribuer une adresse IP au switch sur le VLAN de gestion, le numéro 1.

[18] TRUNK : Multiplexage de VLANs sur un seul lien physique.

```
# ip default-gateway 192.168.1.1
```

La passerelle est configurée sur l'IP du routeur, ce qui donne accès au réseau de l'école et de la même façon, aux machines virtuelles faisant office de serveurs d'authentification et d'autorisation.

3. Systèmes utilisés

3.1 Windows Server 2008 R2

Microsoft Windows Server 2008 R2 est un système d'exploitation qui est prévu pour fonctionner sur des équipements de type serveurs. Il est une évolution majeure par rapport à la version précédente, la version 2003. A mon sens, l'intérêt de ce système d'exploitation est son implémentation des rôles et fonctionnalités. Il permet en effet un nombre impressionnants d'applications dans le système informatique d'une entreprise. Celles qui seront utilisées dans ce travail sont le serveur RADIUS, le NPS, l'émetteur de certificats, ainsi que le rôle de contrôleur de domaine Active Directory. Windows Server 2008 peut aussi faire office, entre autres, de serveur web, serveur applicatif et serveur de bureaux virtuels. C'est donc un outil très puissant.

3.1.1 Laboratoire sur Windows Serveur 2008 R2

Dans ce premier scénario contextuel d'entreprise, nous simulons un système de contrôle d'accès basé sur le produit Microsoft payant, Windows Server 2008 R2. Un premier serveur assure le rôle de contrôleur de domaine, l'autre celui de contrôleur d'accès grâce à la fonctionnalité NPS intégrée dans Windows Server. NPS signifie Network Policy Server, serveur de règles d'accès réseau. Ce deuxième serveur fait aussi office de serveur de remédiation, aidant les clients à mettre leur politique de sécurité à jour pour accéder au réseau. Ceci dans le but d'accepter uniquement des clients non infectés et qui ne présentent aucun danger pour le réseau de l'entreprise.

Un accès au réseau régis par Windows Server 2008 R2 permet les restrictions suivantes :

- S'assurer que le client Windows possède les dernières mises à jour système, ceci par catégorie d'importance de ces dernières (facultatif, recommandé, important).
- S'assurer que le client Windows possède un logiciel anti-virus et qu'il est en fonction.
- S'assurer que le client Windows possède les dernières mises à jour antivirus.

- S'assurer que le client Windows possède un logiciel anti-espion et qu'il est en fonction.
- S'assurer que le client Windows possède les dernières mises à jour antispywares.
- S'assurer que le client Windows possède un pare-feu activé.

Pour ce laboratoire, nous testerons l'état du pare-feu et de l'antivirus, qui sont deux éléments essentiels de sécurité, plus important qu'un anti-spyware.

Il y a trois façons de gérer l'accès au réseau :

- Autoriser un accès complet : les clients répondant aux règles se voient accorder un accès complet au réseau sans restrictions.
- Refuser l'accès complet, accorder un accès limité : les clients ne répondant pas aux exigences sont placés sur un réseau restrictif.
- Autoriser l'accès complet pour une durée limitée : les clients répondant aux exigences ont un accès complet au réseau pour une durée spécifiée à l'avance.

3.1.1.1 Remédiation

3.1.1.1.1 Que se passe-t-il avec les clients non conformes ?

Les clients qui ne sont pas « compliant », autrement dit qui ne répondent pas aux critères définis dans la politique de sécurité du réseau, sont placés sur un réseau de quarantaine et peuvent être sujet à remédiation. Cela veut dire que l'on va leur permettre de se retrouver, manuellement ou automatiquement, en accord avec la politique de sécurité qui leur permettrait un accès complet. Pratiquement dans notre cas, le client est informé par Windows que le NPS a détecté que l'état de son pare-feu est désactivé et qu'il doit y remédier. L'utilisateur peut alors choisir de le réactiver d'un seul clic et de retrouver un accès autorisé. Dans le cas où la règle définie sur le serveur nécessite un programme antivirus, le client Windows va également en proposer le téléchargement depuis une page web (intranet). Une fois le programme installé, le client retrouve son droit à un accès complet automatiquement.

3.1.1.2 Surveillance continue

3.1.1.2.1 Que se passe-t-il avec les clients qui ne répondent plus aux exigences ?

Le NAP surveille constamment l'état des machines afin de pouvoir leur couper l'accès en cas de violation de la stratégie de sécurité. Ceci va être démontré par la désactivation du pare-feu sur la machine de test. Lorsque le client ne répond plus aux exigences, il est immédiatement averti par un message de son système d'exploitation

qui lui expose les faits et lui demande de prendre une décision afin de remédier à la situation. Son accès réseau est instantanément dégradé pour un accès restrictif.

3.1.1.3 Configuration du contrôleur de domaine

Pour ce labo, nous créons un contrôleur de domaine pour le domaine « bachelor.ch », nom choisi arbitrairement à titre d'exemple. Ce serveur fait également office de serveur DNS et de global catalog (annuaire d'objets Active Directory).

La première étape est d'installer le système d'exploitation, Windows Server 2008 R2, sur une nouvelle machine virtuelle. Cette machine possède une interface réseau virtuelle qui est configuré pour se comporter comme une interface réseau physique (mode bridge/pont).

La deuxième étape consiste à installer Active Directory et le service DNS. Pour cela, il faut exécuter la commande « dcpromo » dans une invite de commandes et suivre l'assistant pas à pas.

- Créer un nouveau domaine dans une nouvelle forêt
- Configurer le contrôleur de domaine comme serveur DNS
- Définir un mot de passe de restauration
- Redémarrer quand cela est demandé

Pour pouvoir utiliser une authentification sécurisée avec PEAP, le Network Policy Server a besoin d'un certificat qu'il puisse envoyer aux clients. Ce certificat doit être délivré par une autorité de confiance, en l'occurrence notre contrôleur de domaine. Pour faire de notre contrôleur de domaine une autorité de certification (root CA), il faut lui ajouter le rôle « Active Directory Certificate Services » avec les options par défaut.

Nous créons ensuite un nouveau compte utilisateur dans Active Directory. Celui-ci va être utilisé pour ouvrir une session Windows sur notre machine client. Il faut également l'ajouter au groupe « domain admins » pour qu'il puisse servir à rejoindre le domaine.

Nous allons créons pour la suite, un groupe de sécurité auquel va s'appliquer la politique de sécurité sur la santé de la machine. Nous ne voulons appliquer la politique de sécurité qu'aux ordinateurs de notre choix. Pour se faire, nous nous rendons dans « Active Directory Users and Groups » pour créer ce groupe, appelons le « clients NAP ».

3.1.1.4 Configuration du Network Policy Server

Pour ce laboratoire, nous déployons un deuxième serveur qui assure le rôle du contrôleur d'accès. Il est cependant possible d'utiliser un seul et même serveur en lieu et place de deux, si l'entreprise ne dispose pas de serveurs en suffisance. La séparation reste toutefois préférable pour assurer un fonctionnement optimal et ne pas surcharger le contrôleur de domaine.

En premier lieu, il se voit attribuer une IP dans le même sous-réseau que le contrôleur de domaine ainsi qu'une adresse de serveur DNS correspondant à celle du DC.

La deuxième chose à faire est de joindre le NPS au domaine crée plus tôt, bachelor.ch. Ceci se fait dans le panneau de configuration, dans les propriétés du système et nécessite les identifiants administrateurs.

Pour que le NPS assure son rôle de serveur d'accès, il faut bien sûr installer le rôle NPS. Cela se fait dans « Server Manager », « Add a role ». L'assistant se lance et il suffit de suivre les instructions pour installer le rôle nécessaire.

Nous allons utiliser des GPO (Group Policy Objects) pour spécifier les règles d'accès s'appliquant aux clients. Pour se faire, il faut installer la fonctionnalité de management des group policy. Rendez-vous dans le « Server Manager » sous l'option « Add Features » pour ouvrir l'assistant d'installation d'une nouvelle fonctionnalité.

La prochaine étape pour permettre l'authentification sécurisée avec PEAP est d'obtenir un certificat qui puisse être utilisé dans la communication avec les clients. Ce certificat est bien sûr émis par notre autorité de certification, le contrôleur de domaine. Cela se fait par le biais de la « Microsoft Management Console ». Il faut ajouter le « Snap-in » des certificats. Il apparaît ensuite dans la console. Dans l'arborescence de celui-ci se trouve l'onglet « Personal », il faut faire un clic-droit sur cet élément et sélectionner l'option de demande d'un nouveau certificat. L'assistant d'enregistrement d'un certificat se lance alors. A la fin de l'opération, un message notifiant la réussite devrait apparaitre.

3.1.1.4.1 Système de validation de santé

Pour la suite, il nous faut configurer notre NPS comme « Health Policy Server » que je traduirais par serveur de règles de santé. C'est cet élément qui va permettre la vérification de la conformité du système client par rapport aux règles de sécurité définies pour le niveau de sécurité acceptable d'une machine souhaitant avoir accès aux ressources. Cela se fait à l'aide de l'assistant NAP (Network Access Protection)

qui va nous configurer les polices d'accès qui correspondent à notre infrastructure réseau. Pour le démarrer il faut taper « nps.msc » dans une invite de commandes. Cela ouvre une console de management avec le snap-in NPS. Dans les détails de ce dernier, sous « Standard Configuration » se trouve l'option pour configurer le NAP. L'assistant s'ouvre alors.

Le premier choix à faire est de sélectionner le type de connexion au réseau à utiliser. Nous sélectionnons « IEEE 802.1X (Wired) ». En effet, nous utilisons bien le 802.1X câblé. Sur la page suivante il faut ajouter le ou les switch(s) authentificateur(s). Dans le cadre ce laboratoire nous n'avons qu'un seul système authentificateur. C'est donc dans une fenêtre de nouveau client RADIUS que nous ajoutons l'IP du switch ainsi que son mot de passe secret. L'affichage de la page d'assistant sur la méthode d'authentification doit afficher le certificat utilisé ainsi que l'utilisation du type EAP suivant : PEAP-MSCHAPv2. Dès la fenêtre suivante, nous pouvons configurer des attributs supplémentaires à envoyer au système authentificateur en plus de la simple autorisation d'accès. Nous allons définir une attribution de sous-réseau virtuel (VLAN), tout d'abord pour les clients qui sont conformes. L'option à sélectionner se nomme « Configure Traffic Controls ». On peut ensuite choisir de définir la configuration des attributs RADIUS pour l'accès total au réseau et pour l'accès restreint. La méthode reste la même pour les deux options. Il faut configurer les attributs RADIUS suivants :

- Tunnel-Type : VLAN
- Tunnel-Medium-Type : 802
- Tunnel-Pvt-Group-ID : 3 (VLAN conforme) et 2 (VLAN restrictif).

Nous verrons par la suite que ces paramètres sont les mêmes utilisés pour la configuration de Cisco ACS. L'assistant de configuration du NAP est maintenant terminé.

3.1.1.4.2 Modifier les règles de sécurité

Pour pouvoir spécifier sur quels critères de santé informatique nous allons évaluer le client Windows, il faut configurer les paramètres du système de validation. Ceci se fait dans la console d'administration du Network Policy Server, sous l'onglet « Network Access Protection ». Il faut ensuite étendre l'arbre jusqu'aux « Settings » du « Windows Security Health Validator », comme indiqué dans la figure ci-dessous. On peut définir plusieurs configurations et/ou modifier la configuration de base. Nous

allons modifier la « Default Configuration ». Le panneau est séparé en 2 options : Windows XP et Windows 7/Vista. Ensuite on peut activer ou désactiver la vérification du pare-feu, de l'antivirus et de l'antispyware (avec ou sans prendre en compte les mises à jour). L'exemple se trouve à la page suivante.

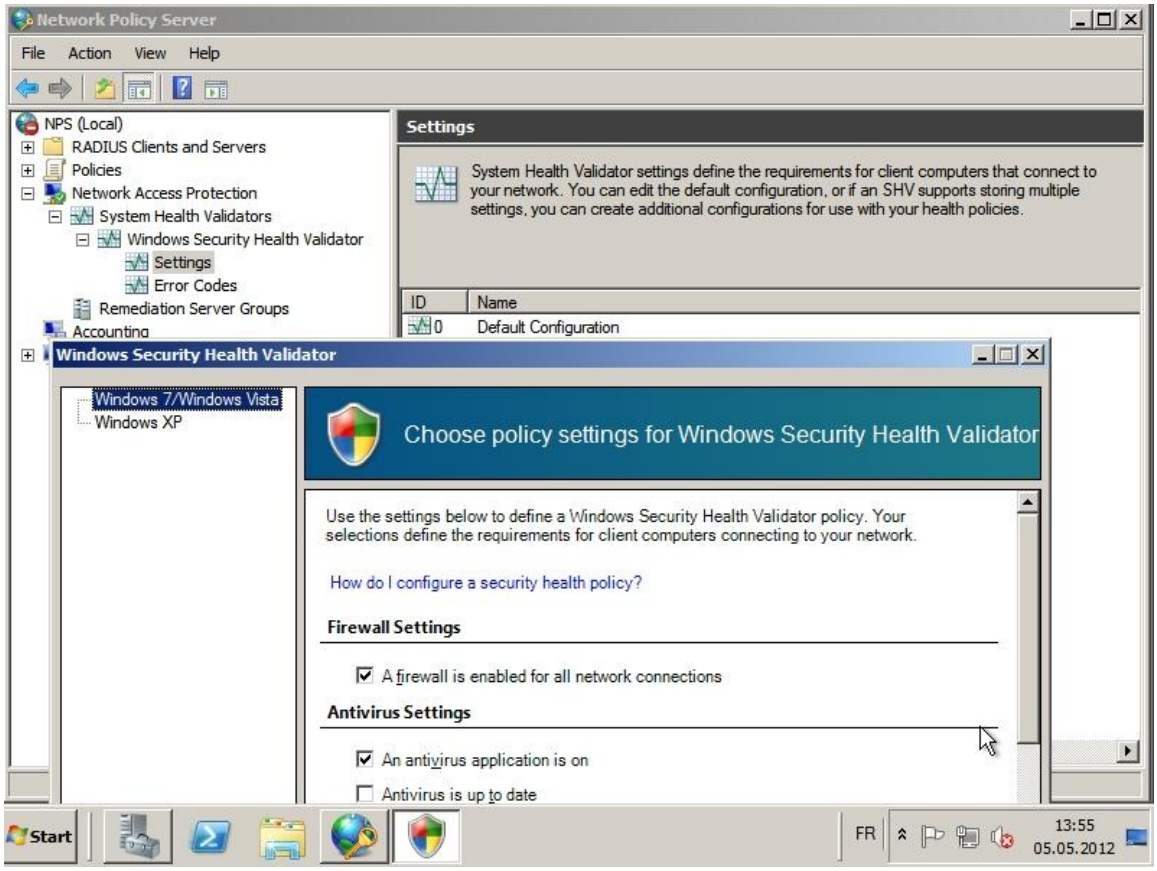

Figure 6: Windows Security Health Validator

Il est également possible de vérifier que le client Windows est à jour au niveau des patchs émis par Microsoft. Le choix peut-être fait sur le niveau d'importance des mises à jour. Il existe 4 niveaux. Le premier est « faible est au-dessus » : Toutes les mises à jour doivent être faites sans exception. Le deuxième niveau possible est « modéré et au-dessus » : Les mises à jour d'importance moyenne, importantes et critiques doivent être installées. Le niveau « Important et au-dessus » : Toutes les mises à jour importantes et critiques. Dernier niveau « Critique seulement », seules les mises à jour critiques doivent être faites. Il est bon de préciser que sur la capture d'écran, conformément à notre labo, nous cochons l'obligation d'avoir un pare-feu activé pour toutes les connexions de l'ordinateur ainsi qu'un antivirus installé. Nous pourrions envisager d'obliger le client à avoir les dernières définitions de signatures de virus, mais il faudrait dans ce cas créer des Access List permettant de contacter les serveurs

de mises à jour correspondants tout en ayant un accès restreint au réseau.

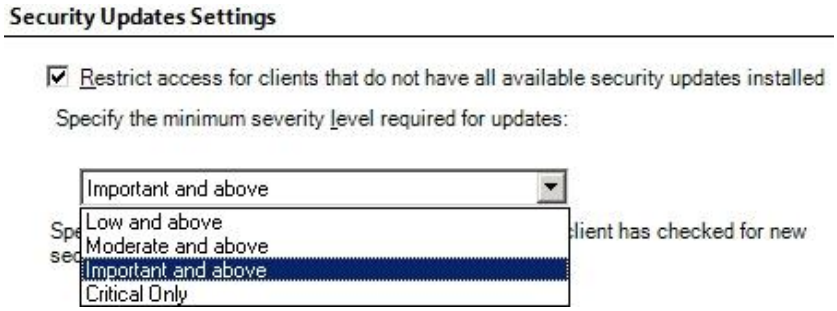

Figure 7: Security Updates Settings

La prochaine étape consiste à forcer les clients que nous sélectionnons à être en accord avec la politique de sécurité, tandis que les autres clients comme les ordinateurs fixes connus et appartenant à l'entreprise pourraient par exemple ne pas être soumis aux mêmes règles. Nous allons bien sûr aussi exclure les serveurs de la manipulation. Il faut créer une GPO[19] que nous nommons « NAP client settings ». Ceci se fait en exécutant « gpme.msc » qui ouvre la console de management avec le snap-in de Group Policy Management. Il faut ensuite faire un clic-droit sur « Group Policy Objects » et sélectionner « new » pour créer une nouvelle GPO que l'on nomme « NAP client settings ». En effet, elle contiendra les paramétrages qui sont spécifiques aux clients soumis à notre politique de sécurité.

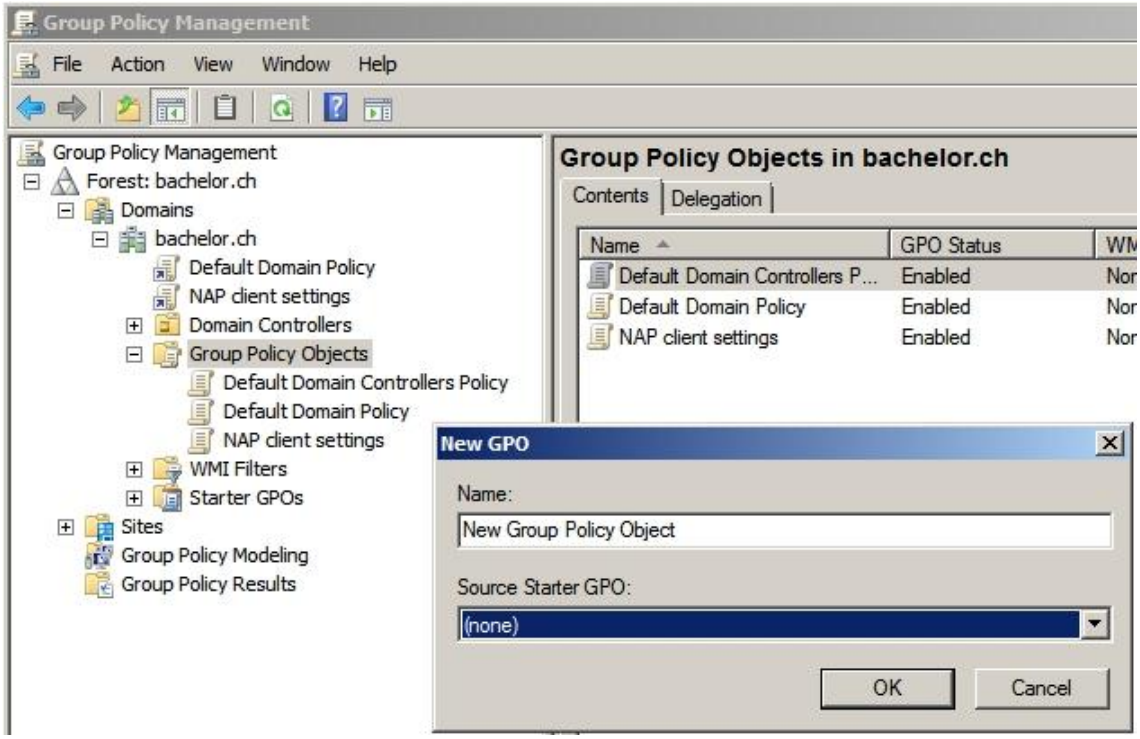

Figure 8: New Group Policy Object

[19] Group Policy Object : Stratégie de groupe

Dans cette GPO, il nous faut filtrer en précisant que seuls les ordinateurs du groupe « NAP client computers » seront touchés par ce paramétrage. Sur la capture nous voyons nos deux clients de test qui font bien partie de ce groupe et pour lesquels les paramètres que nous allons configurer vont s'appliquer.

Figure 9: Security Filtering

Pour définir ce que nous avons besoin, nous allons dans l'édition de cette stratégie de groupe. Premier impératif, mettre le « Wired Autoconfig » sur « enabled ». Ce qui active le service de configuration automatique du réseau.

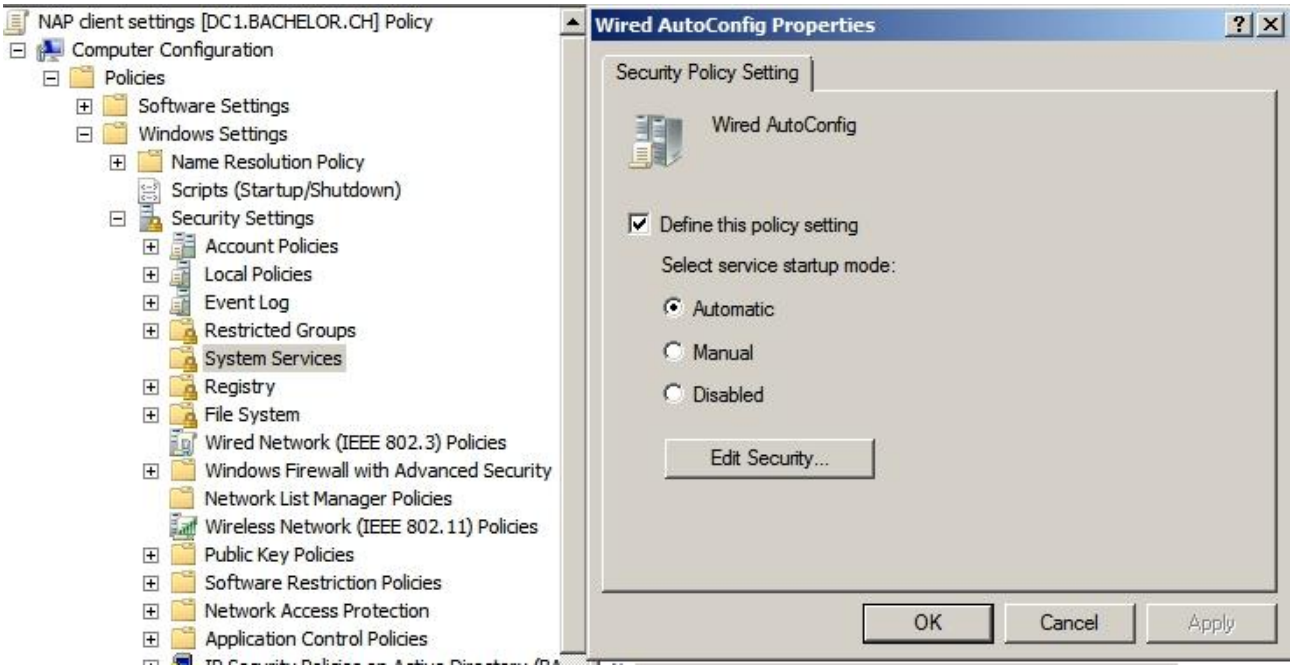

Figure 10: Wired AutoConfig Activation

Deuxième impératif, activer le service de protection d'accès réseau. En effet, c'est lui qui fait tout le travail de contrôle sur le client.

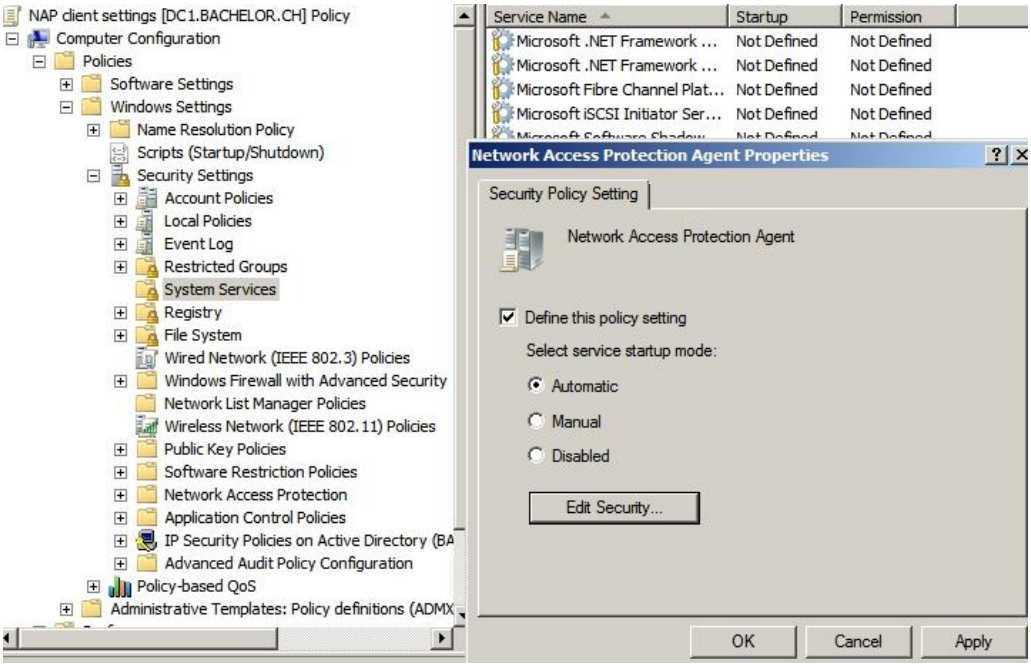

Figure 11: Network Access Protection Agent Activation

Il reste encore à activer le client de quarantaine EAP. Celui-ci fournit la protection d'accès réseau pour les réseaux authentifiés avec EAP, notamment avec 802.1X. Il est donc indispensable pour mettre en quarantaine le client non conforme.

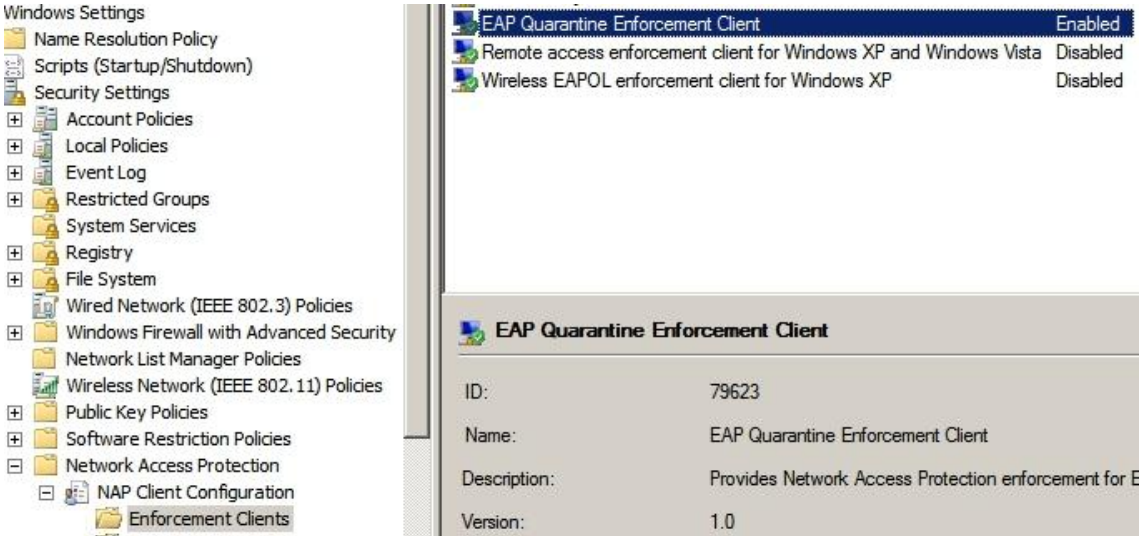

Figure 12: EAP Quarantine Enforcement Client

Il ne reste plus qu'à forcer l'activation du centre de sécurité Windows, qui s'occupe de gérer le pare-feu, l'antivirus et l'antispyware et de vérifier si ceux si sont installés, activés et/ou à jour.

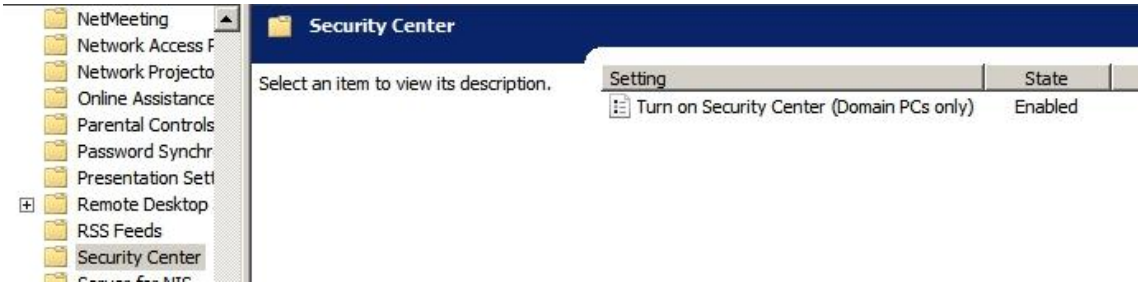

Figure 13: Security Center Activation

3.1.1.5 Configuration du client 802.1x

Le client 802.1x est un ordinateur sous Windows 7 qui désire accéder aux ressources internes à l'entreprise, notamment l'accès à Internet, avec l'authentification basé sur le port. La première étape consiste à joindre le client au domaine Active Directory, pour cela il faut changer sa configuration DNS pour que son serveur DNS soit notre contrôleur de domaine.

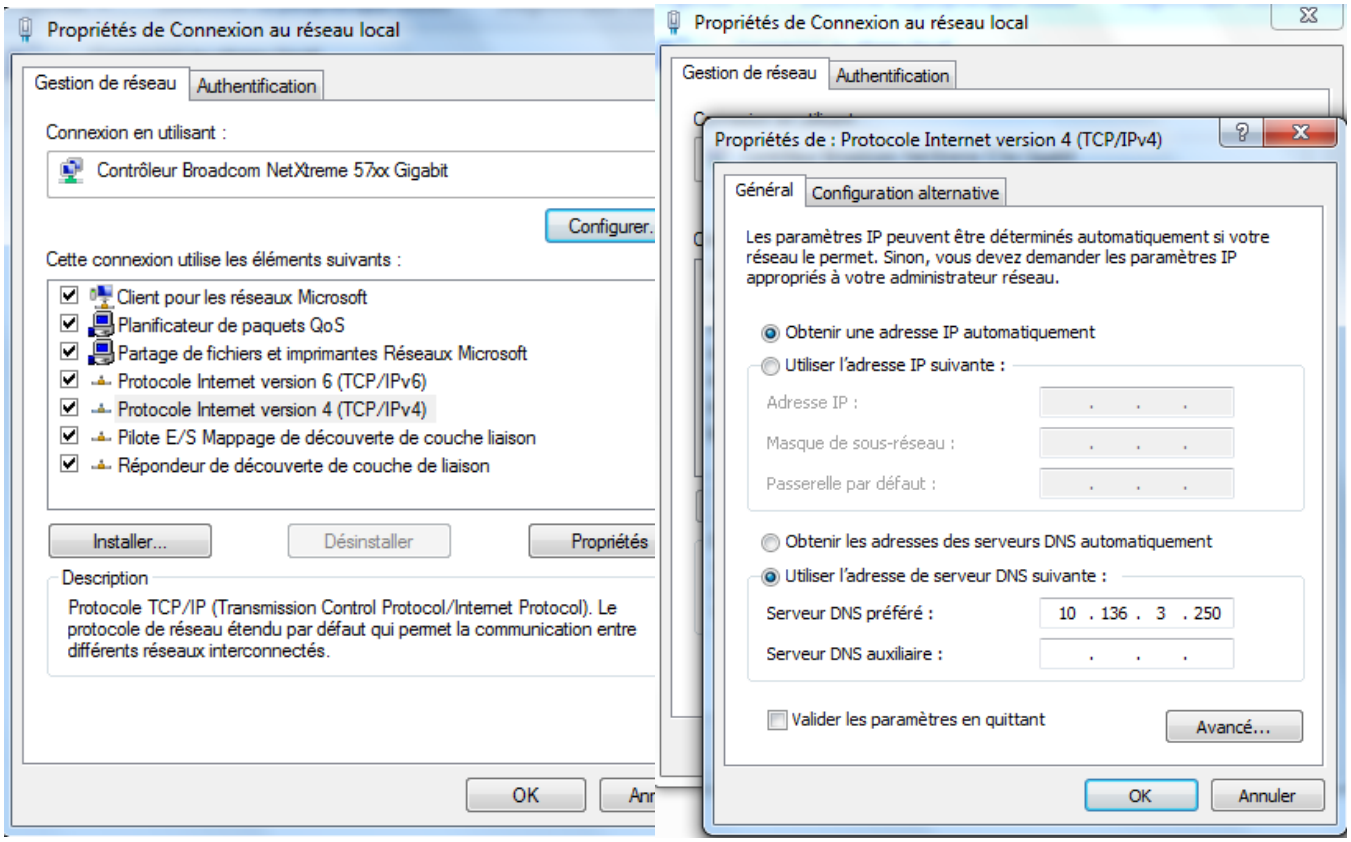

Figure 14: Propriétés TCP/IPv4

Pour l'étape de l'ajout au domaine de l'ordinateur, il est indispensable que la résolution du nom de domaine parte sur le DNS du contrôleur de ce même domaine. Si ce n'est pas le, notre client ne pourra pas rejoindre le domaine. C'est une opération qu'il faut souvent faire en labo, mais dans un contexte entreprise, il est fort possible que la configuration automatique attribuée par le serveur DHCP fasse l'affaire sans problème.

L'ajout du client au domaine se fait dans le panneau de configuration => système => paramètres système avancés => nom de l'ordinateur => modifier.

L'opération suivante peut également se faire AVANT de joindre le client au domaine. Dans « Active Directory Users and Groups », il faut place un nouvel objet ordinateur avec le nom correspondant à l'ordinateur client dans le groupe des clients NAP. Celui-ci sera alors automatiquement lié à cet objet lorsqu'il rejoint le domaine. Si cette opération n'as pas été faite, il faut déplacer le nouvel objet qui devrait être apparu dans le groupe correspondant. Une fois fait, l'ordinateur client peut être redémarré.

Comment vérifier que le client est bien soumis à notre GPO ? Nous allons ouvrir une ligne de commandes et taper :

```
# netsh nap client show grouppolicy
```

La ligne « EAP Quarantine Enforcement Client » devrait être « enabled ». Cela nous permet d'être sûr que le client sera placé en quarantaine si il ne répond pas aux critères de sécurité définis. Il nous faut encore vérifier que son statut est initialisé pour le client. La commande suivante s'en charge :

```
# netsh nap client show state
```

Vérifions que la ligne « EAP Quarantine Enforcement Client » est à « Yes » et nous sommes maintenant sûr que l'ordinateur du client agira en conséquence.

La prochaine étape est de configurer la connexion réseau locale de l'ordinateur pour l'authentification. Ceci peut aussi être fait par le biais d'une GPO mais cela dépasse le cadre de ce travail et la configuration est donc faite directement sur la machine localement. Il faut donc se rendre dans le panneau de configuration Windows, « Centre réseau et partage » puis avec un clic-droit de la souris on accède aux propriétés de la connexion au réseau local, ceci ouvre la fenêtre affichée sur figure de la page suivante.

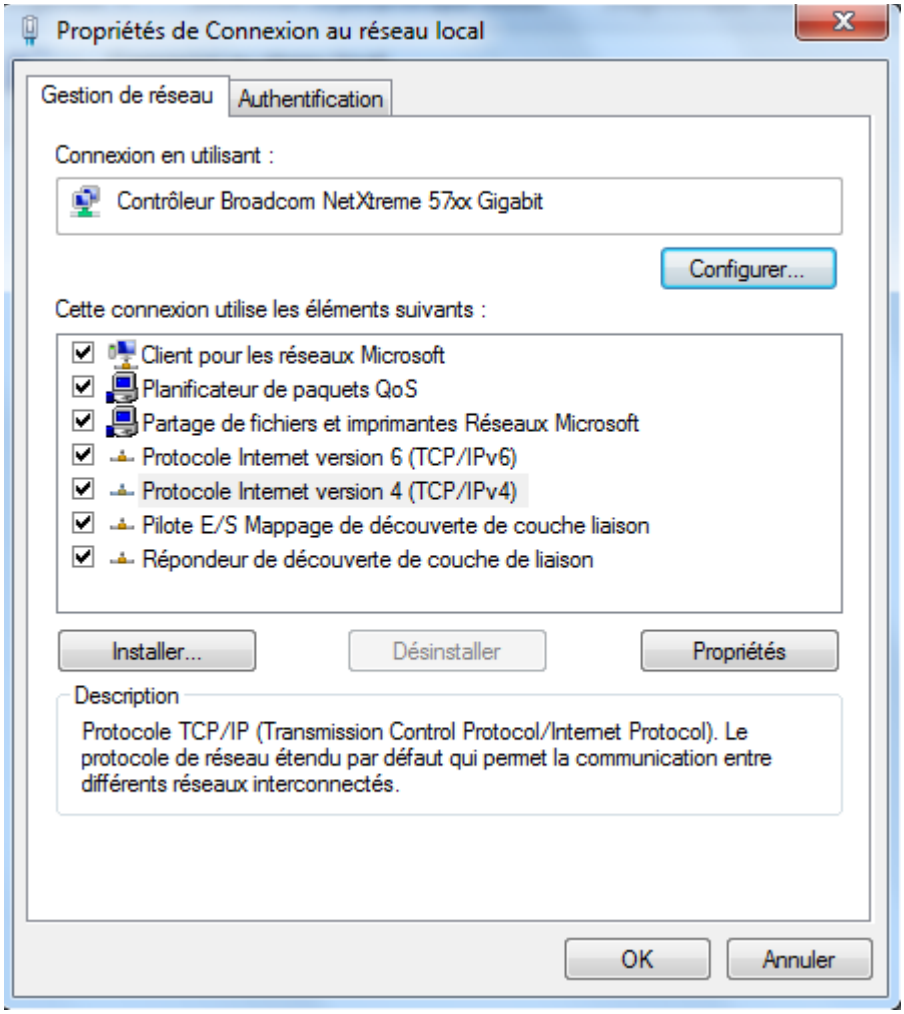

Figure 15: Gestion de réseau

Nous avons déjà réglé l'aspect de la configuration IP, il reste donc à nous rendre sur l'onglet « Authentification » pour choisir nos paramètres et rendre notre test opérationnel. Suite à la page suivante.

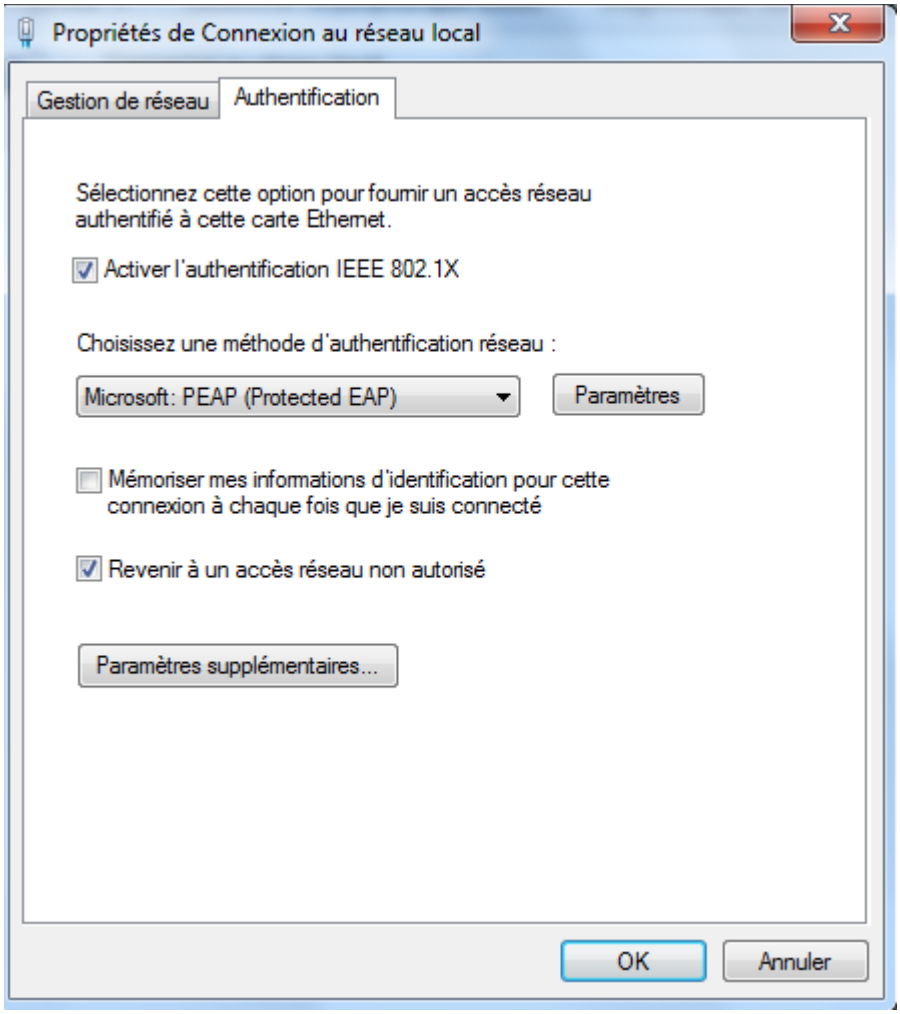

Figure 16: Onglet Authentification

Nous voici donc au cœur du sujet, il faut activer l'authentification 802.1X en sélectionnant la case à cocher correspondante. Nous choisissons PEAP(version Microsoft, soit PEAP-MS-CHAPv2). Contrairement à EAP-TLS ou PEAP-TLS, il n'y a nul besoin d'installer de certificat sur le poste client avant de pouvoir établir une connexion. En premier lieu, un tunnel sécurisé est créé grâce au certificat du serveur, puis la négociation de la communication se fait au niveau du couple user/password. Il faut bien sûr cocher « Revenir à un accès réseau non autorisé », sans quoi un client malveillant peut faire mine de répondre aux règles de sécurité puis désactiver par la suite sont antivirus ou pare-feu et mettre en danger le réseau sain. Il est dans ce cas-là bien sûr plus logique de contraindre ce paramètre par le biais d'une GPO.

Nous nous intéressons ensuite aux paramètres de PEAP. Capture d'écran à la page suivante.

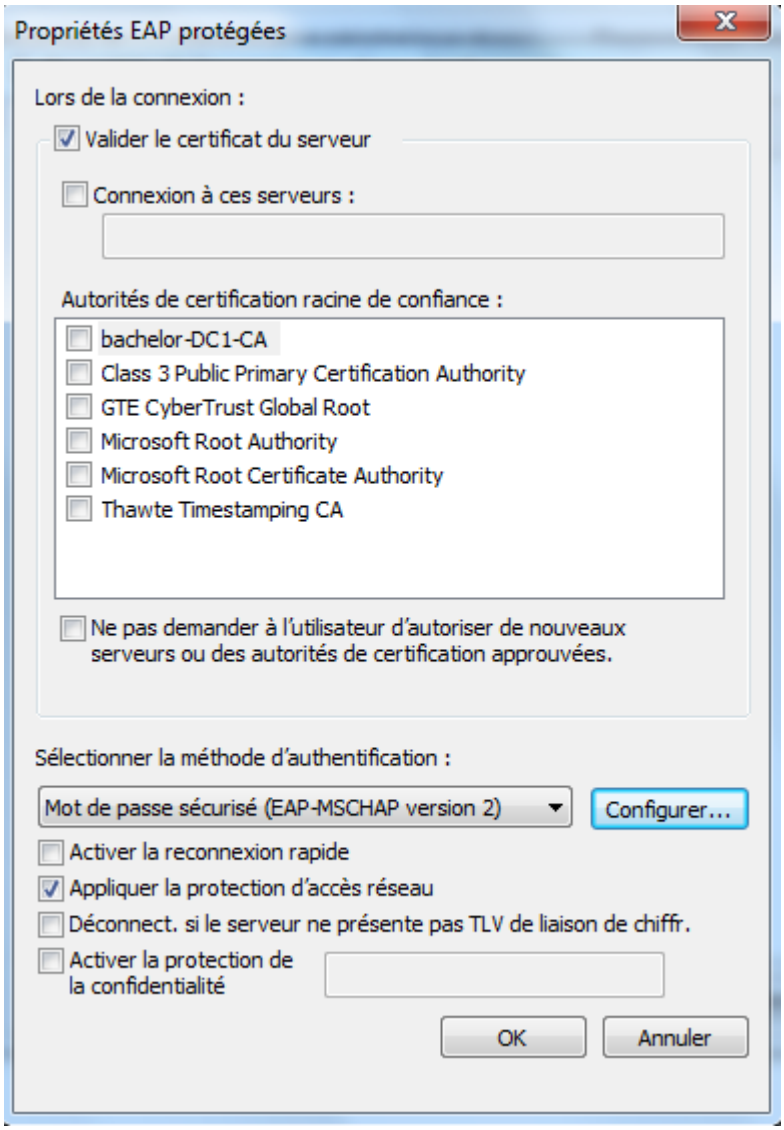

Figure 17: Propriétés PEAP

La première coche à mettre est celle de la validation du certificat du serveur. Le NPS possède un certificat émis par le contrôleur de domaine et il s'agit au client de l'utiliser pour construire leur relation de confiance. Il faut aussi préciser que nous utilisons la variante de PEAP-EAP-MSCHAPv2 (dans configurer, vérifier que l'option utiliser mon login Windows est activée) et appliquer la protection d'accès réseau vu que c'est le but de notre démonstration.

C'est tout pour la partie client, la démonstration peut commencer.

3.1.1.6 Test de la configuration

Le test peut maintenant commencer. Notre client démarre son ordinateur et ouvre sa session sur le domaine bachelor.ch avec un compte utilisateur répertorié dans la base Active Directory.

3.1.1.6.1 Situation de départ

La session est ouverte. Le client n'a pas d'antivirus installé. Son pare-feu Windows est également désactivé. Pour assurer la sécurité du réseau, l'accès accordé est limité (comme le montre la figure 3). Nous lui autorisons tout de même un accès qui est restreint, il est isolé sur un réseau virtuel qui ne possède pas d'autorisation pour accéder aux ressources d'entreprise. Ceci est simulé dans le laboratoire par le fait que ce VLAN n'as pas d'accès au réseau de l'école. Son adresse privée n'as de droit d'accès sur aucunes ressources si ce n'est l'accès web au serveur de remédiation. Il a donc la possibilité de se mettre en conformité avec la politique de sécurité.

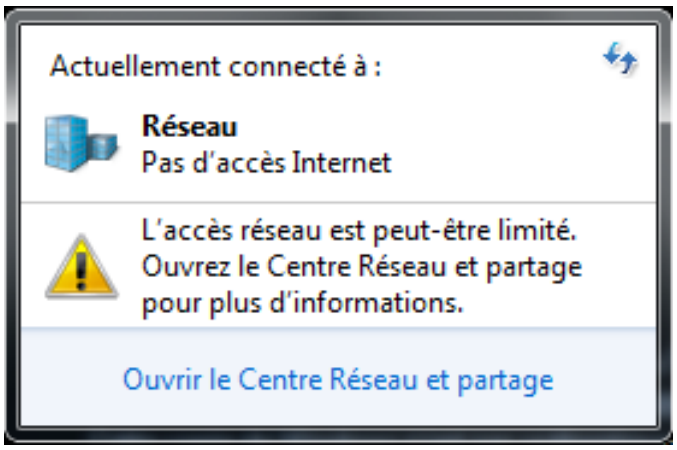

Figure 18: Accès réseau limité

Pour se mettre en conformité, le client suit les instructions qui s'affichent sur son écran. En ouvrant le centre réseau et partage, l'écran suivant s'affiche.

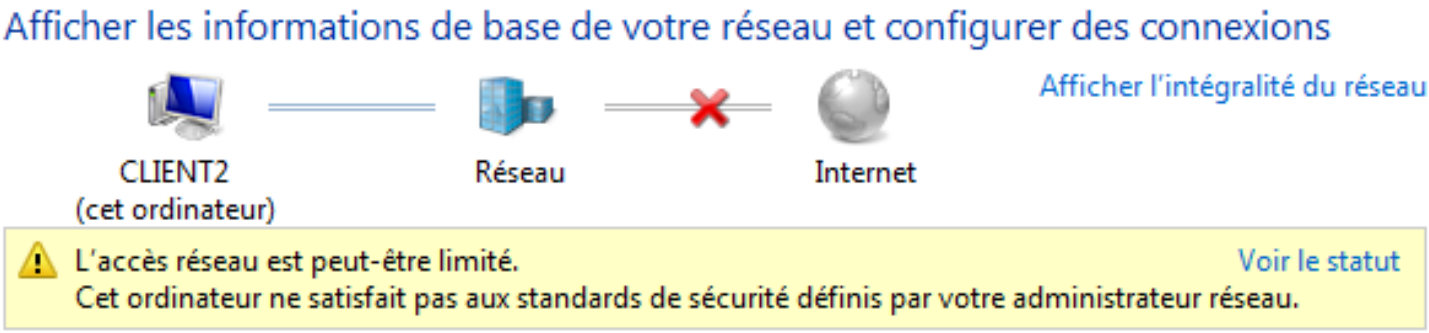

Figure 19: Client non conforme à la politique

En cliquant sur « Voir le statut », le client peut voir les raisons pour lesquelles sont système n'est pas conforme aux règles de sécurité du réseau.

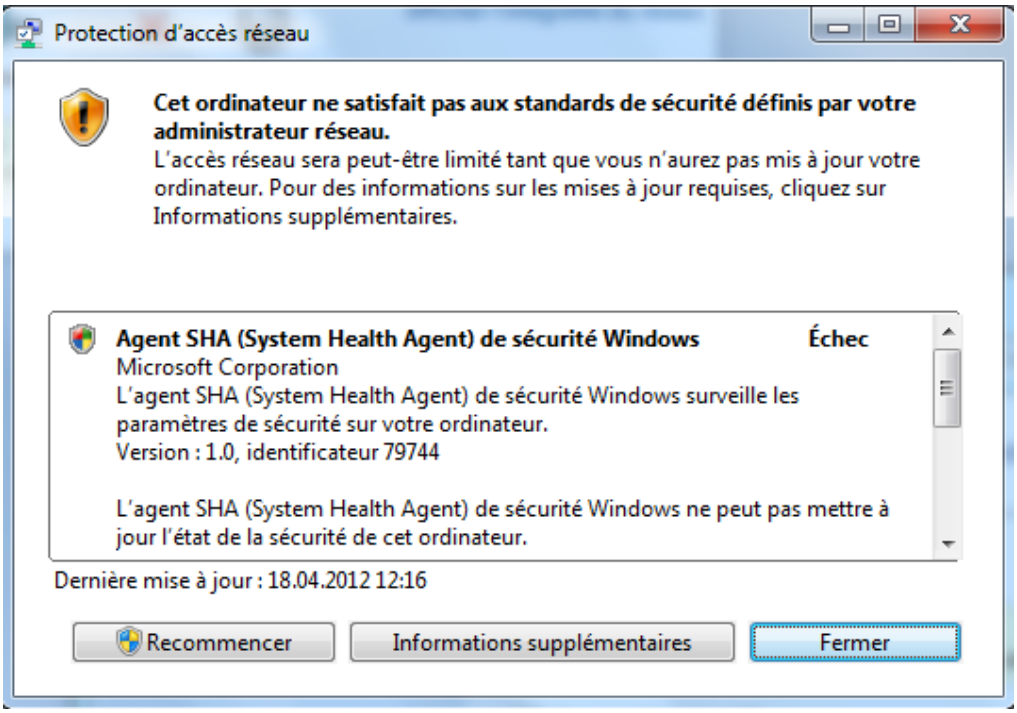

Figure 20: System Health Agent

Nous voyons sur la figure ci-dessus que c'est l'agent de sécurité Windows qui s'occupe de vérifier en tout temps la conformité du client et de transmettre les résultats de son analyse au serveur. Voyons tout d'abord le cas où le pare-feu du client est désactivé. Le message suivant s'affiche.

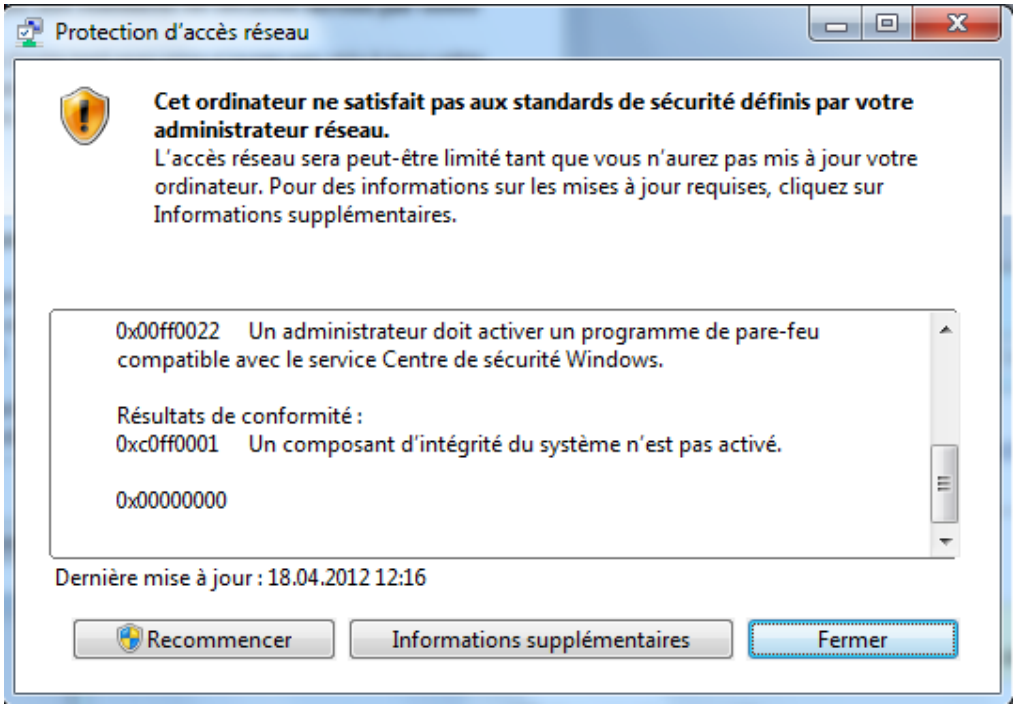

Figure 21: Pas de pare-feu activé

Un simple clic sur « Recommencer » avec les droits d'administrateur sur la machine permet de réactiver le pare-feu pour passer en mode autorisé. Voyons maintenant le cas où la politique de sécurité exige un logiciel antivirus sur la machine client.

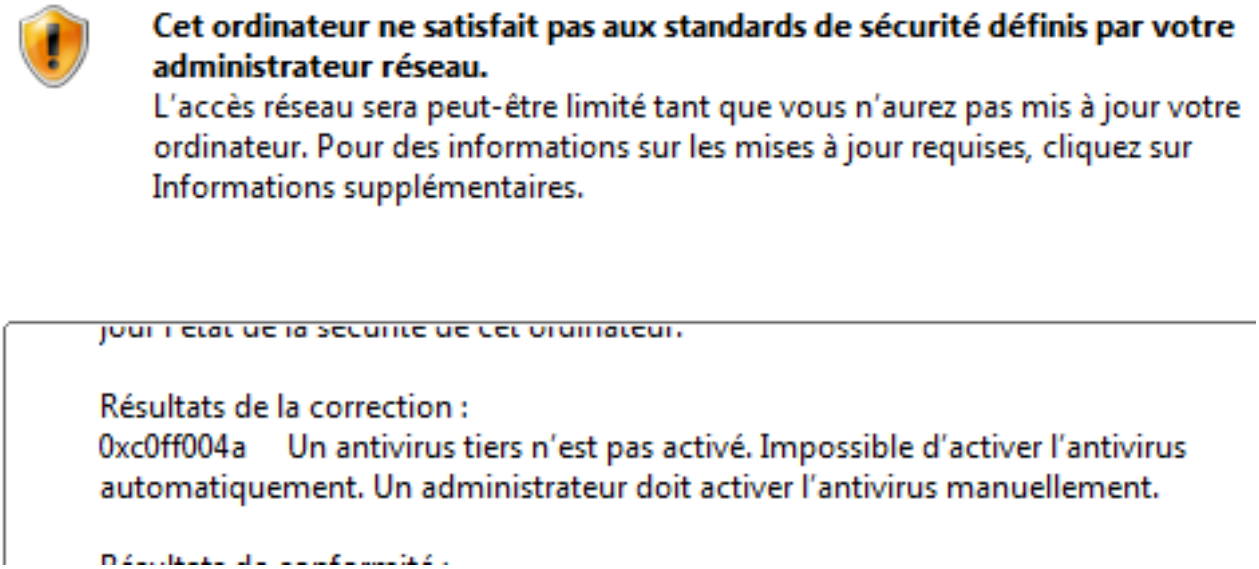

Figure 22: Antivirus non présent ou activé

Il faut dans ce cas-là cliquer sur « Informations supplémentaires » (cf. Fig.21), ce qui a pour effet d'ouvrir la page de remédiation qui peut prendre diverses formes, pour ce laboratoire elle ressemble à ceci.

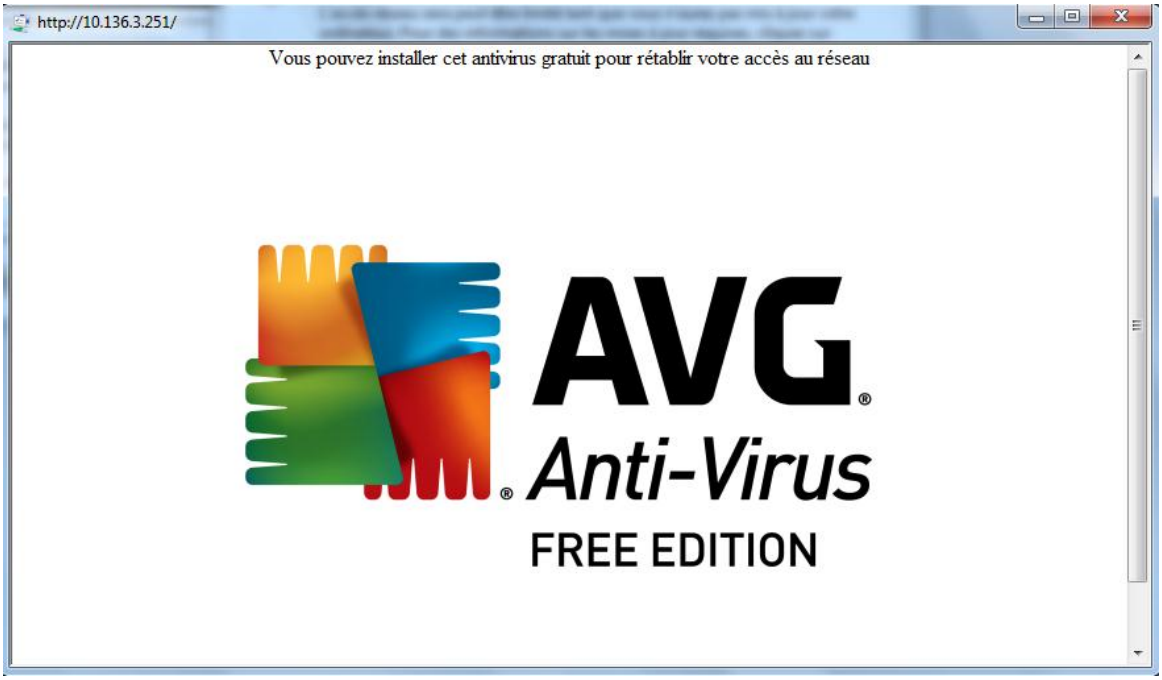

Figure 23: Page de remédiation

Le client peut ensuite télécharger l'antivirus depuis le serveur de remédiation et l'installer, après quoi il sera autorisé à accéder au réseau. Les étapes en 3 images.

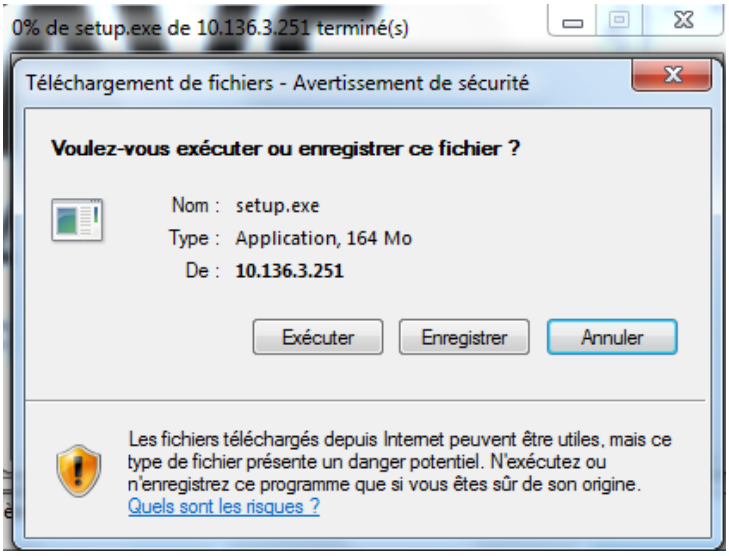

Figure 25: Avertissement de sécurité

Figure 24: Installation de l'antivirus

Voyons maintenant en détails et concrètement les accès disponibles pour le client, avant et après installation de l'antivirus. Avant installation, le client est dans le VLAN 2, notre VLAN restrictif.

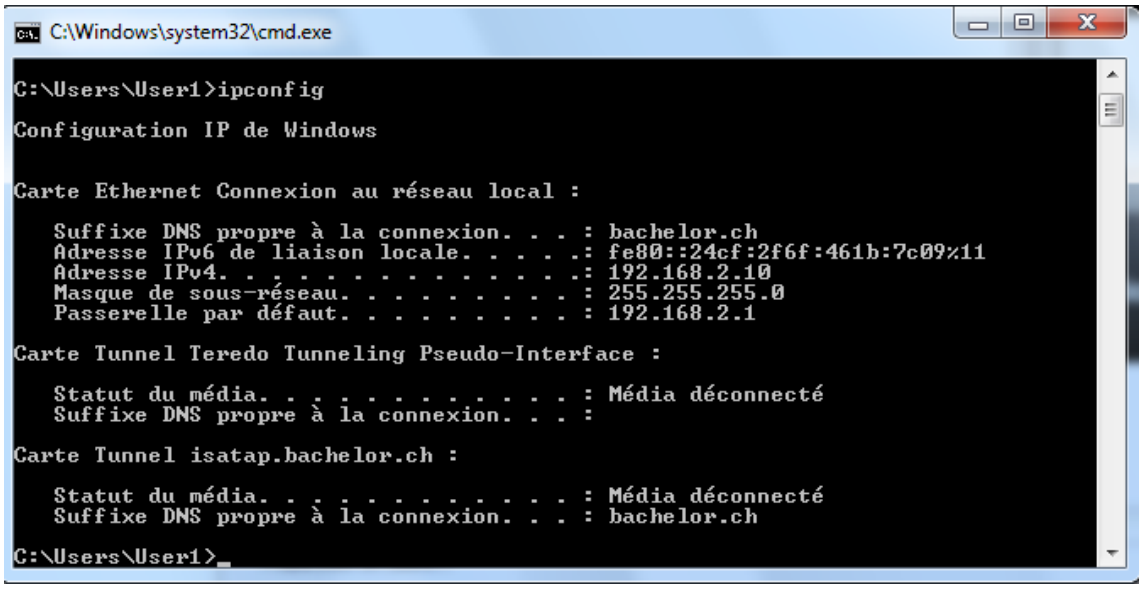

Figure 26: ipconfig VLAN 2

L'adresse qui lui est attribuée fait donc partie du sous-réseau correspondant. Celui-ci n'a pas d'autorisation pour un accès aux ressources autre que le serveur de remédiation. D'ailleurs Internet ne fonctionne pas.

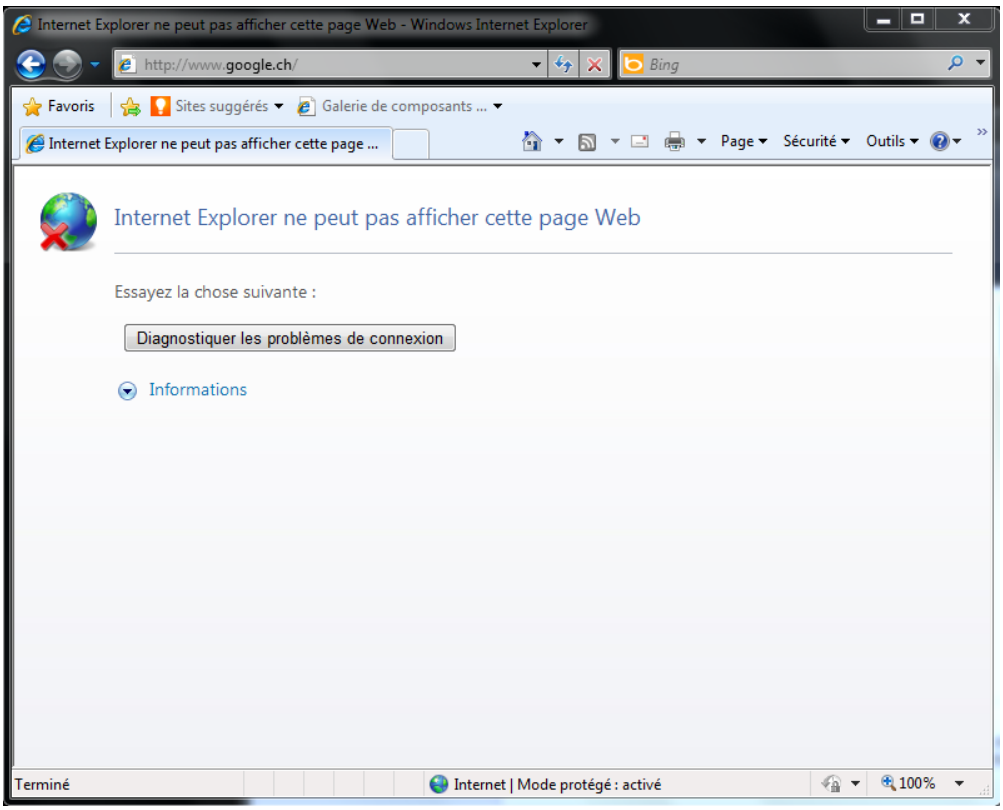

Figure 27: Accès Internet indisponible

Ensuite a lieu la fameuse remédiation dont nous avons détaillé la procédure plus haut. Immédiatement après l'activation de l'antivirus, le client avertit le système authentificateur de son nouvel état et communique ensuite avec le serveur d'authentification pour obtenir une nouvelle autorisation. Le système authentificateur voit l'autorisation délivrée par le serveur et l'applique donc à notre client en le basculant sur le VLAN 3, le VLAN autorisé.

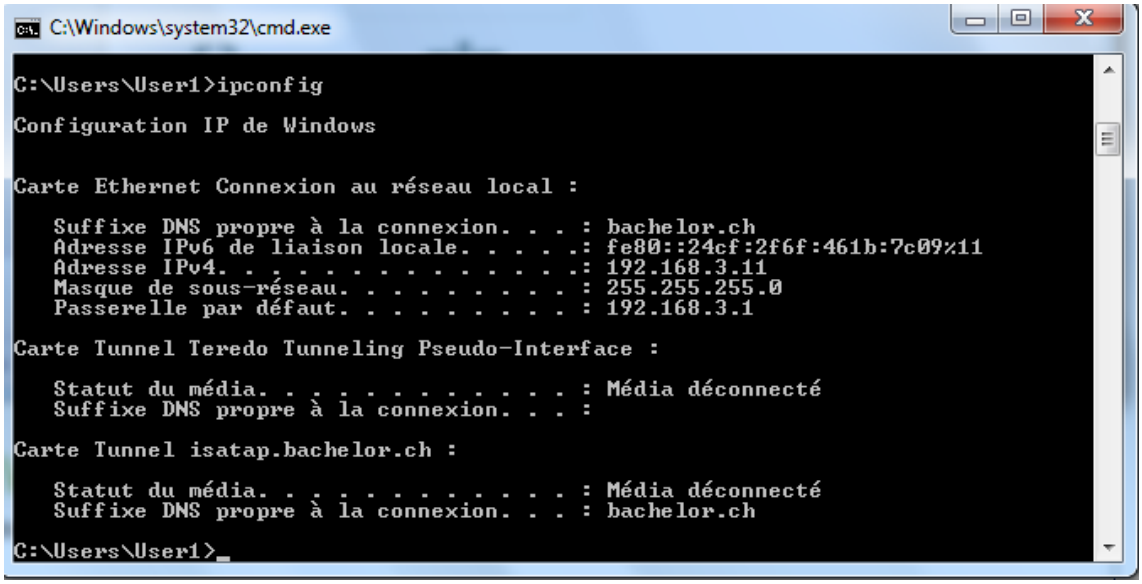

Figure 28: ipconfig VLAN 3

L'adresse IP est bien celle du sous-réseau correspondant au VLAN 3. L'accès à Internet et aux autres services est immédiatement rétabli.

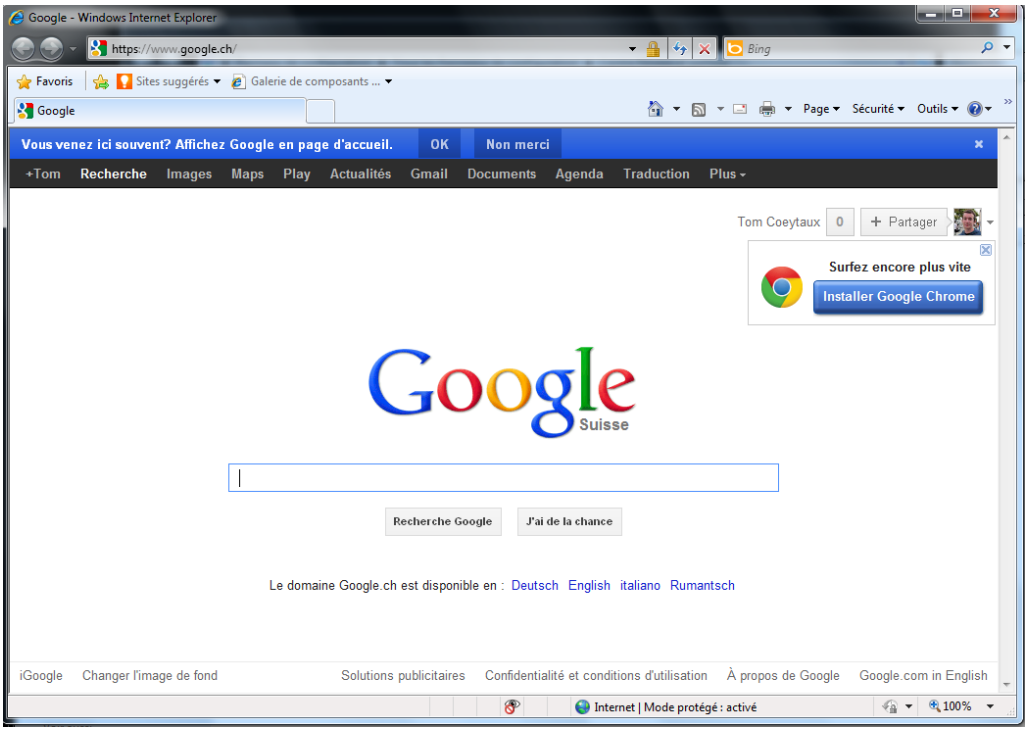

Figure 29: Accès Internet rétabli

3.2 Cisco Secure Access Control System 5.x

Cisco Secure ACS est disponible sur le marché en Rack 1U avec une distribution CentOS sur laquelle le logiciel est préinstallé. Il est également disponible sous forme d'image de système d'exploitation pour VMWare pour une exploitation dans un environnement virtualisé. C'est cette dernière version qui est utilisée, en version d'évaluation gracieusement accordée par Cisco. En effet, je n'ai pas à ma disposition tout l'éventail de solutions Cisco, celui-ci ayant un prix raisonnablement inabordable pour une petite entreprise. Le produit généralement utilisé par les PME se nomme ACS express, le logiciel testé avec certaines restrictions en plus. Ce logiciel que je vais utiliser, diffère de « Cisco Network Admission Control » du fait qu'il ne propose pas de vérification de l'état de santé (du point de vue informatique) du client souhaitant s'authentifier, ni de système de quarantaine et remédiation. Contrairement à Windows Server, c'est un serveur RADIUS (ou TACACS+) uniquement, mais avec des fonctionnalités étendues. C'est donc d'autres restrictions en fonction d'autres critères que nous pourrons appliquer grâce à Cisco Secure ACS. En effet, Cisco NAC n'est pas disponible en version à l'essai. De plus, il nécessiterait (dans l'idéal) un écosystème d'équipements Cisco complexes que je ne peux pas me procurer pour ce laboratoire.

ACS journalise les événements ayant lieu sur le réseau. Cet outil possède aussi des fonctions de monitoring, de reporting et de dépannage intégrés, le tout accessible avec l'interface graphique web. Il est spécialement conçu pour offrir un contrôle centralisé des règles d'accès et de l'administration des clients et des équipements réseaux, pour des accès 802.1x sans-fil ou câblés.

3.2.1 Labo Cisco ACS

La configuration du serveur Radius, en l'occurrence Cisco ACS, se déroule en 4 étapes :

- Configurer les ressources réseaux. Soit les systèmes authentificateurs, qui sont les clients qui vont devoir se connecter à notre serveur ACS.
- Configurer les utilisateurs. Externe ou interne. Dans notre cas la base de données Active Directory liée à aller consulter.
- Créer des règles d'accès
- Appliquer les règles d'accès

Pour créer des règles d'accès, plusieurs éléments sont à notre disposition. Tout d'abord les informations d'identité. Ces informations proviennent souvent d'un

répertoire sous la forme d'un AD ou d'un LDAP mais peuvent aussi être définies dans Cisco ACS de manière fixe et isolée d'un composant extérieur.

Le deuxième élément utilisé consiste en une restriction, qu'elle soit basée sur un aspect temporel, sur un périphérique particulier ou toute autre condition que l'on souhaite observer avant de mettre en route la police d'accès établie.

Troisième et dernier élément indispensable, la permission. Qui permet de définir les autorisations accordées dans chaque situation, pour chaque règle d'accès. Cela se concrétise avec, par exemple, une attribution de VLAN, un privilège d'accès IOS ou une activation d'ACL.

La règle d'accès fonctionne ensuite avec une combinaison de ces trois éléments. Elle prend la forme suivante : si condition, alors autorisation. La condition peut prendre la forme d'une restriction ou d'une identité, ou d'une combinaison des deux. L'autorisation quant à elle définit une ou plusieurs permissions qui sont accordés pour cette règle d'accès.

3.2.1.1 En pratique

La première étape de la mise en pratique commence par le déploiement de la machine virtuelle ACS. J'ai pu obtenir une version d'évaluation de 90 jours afin de procéder à une configuration de test et déterminer la valeur du produit. La mention apparait sur la page d'accueil de l'interface web.

Figure 30: Cisco Secure ACS Dashboard

3.2.1.2 Configuration

3.2.1.2.1 Client 802.1x

En premier lieu, le client de test qui doit s'authentifier doit être configuré. C'est déjà le cas car la configuration de notre dernier labo est compatible avec celui-ci. En effet, nous utilisons un utilisateur de notre domaine AD pour s'authentifier. Les seules modifications portent sur les « quarantine check » et la validation du certificat du serveur qui ne sont pas utilisés dans ce labo ACS.

3.2.1.2.2 Modification de la configuration du switch

Quant au switch Catalyst qui est notre système authentificateur, seul l'adresse IP du serveur Radius est à modifier, ceci se fait très simplement avec la commande :

```
# radius-server host 10.136.3.25x auth-port 1812 acct-port 1813 key 7 s3cr3t
```

3.2.1.2.3 Configuration du serveur ACS

```
Press 'Ctrl-C' to abort setup
Enter hostname[]: ACS
Enter IP address[]: 10.136.3.252
Enter IP default netmask[]: 255.255.252.0
Enter IP default gateway[]: 10.136.0.21
Enter default DNS domain[]: 10.136.3.250
Enter default DNS domain[]: bachelor.ch
Enter Primary nameserver[]: 10.136.3.250
Add/Edit another nameserver? Y/N : y
Enter Secondary nameserver[]: 160.53.236.30
Add/Edit another nameserver? Y/N : n
Enter username[admin]:
Enter password:
Enter password again:
Bringing up network interface...
Pinging the gateway...
Pinging the primary nameserver...
Do not use 'Ctrl-C' from this point on...
Appliance is configured
Installing applications...
Installing acs ...
```

Figure 31: Initial Setup

Comme nous pouvons le voir sur les captures ci-dessus et ci-contre, une des premières étapes de l'installation de la machine virtuelle ACS est la configuration basique : adresse IP, masque de sous-réseau et surtout serveur de noms. J'ai tout d'abord mis celui du réseau de l'école, avant de me rendre compte que je devais avoir accès aux utilisateurs d'Active Directory situés sur mon domaine Bachelor.ch. Pour pouvoir résoudre ce nom de domaine, il faut que le serveur de nom sur ma machine Cisco ACS soit configuré sur le serveur DNS du contrôleur de domaine (dans mon cas précis). Ceci se fait, dans un style similaire à Cisco IOS et lorsque l'assistant n'est pas activé, avec les commandes indiquées sur la figure 32 de la page suivante.

```
ACS/admin# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ACS/admin(config)# ip name-server 10.136.3.250
Name Server was modified. You must restart ACS.
Do you want to restart ACS now? (yes/no) yes
Stopping ACS.
Stopping Management and View.....................
```

Figure 32: ip name-server and reload

3.2.1.2.4 Configurer les ressources réseaux

Il nous faut encore définir notre périphérique authentificateur qu'est le switch, l'écran pour faire cette manipulation est présenté sur la prochaine capture :

Figure 33: Device Categories

Un aspect intéressant de Cisco ACS est de pouvoir définir des catégories d'équipements, sur le modèle parent/enfant et ceci à volonté. Cela permet de bien gérer son parc d'équipement réseaux. Mieux encore, il est possible ensuite de définir un emplacement pour chaque équipement, selon le même principe de catégorisation. Exemple sur cette capture d'écran de l'interface web :

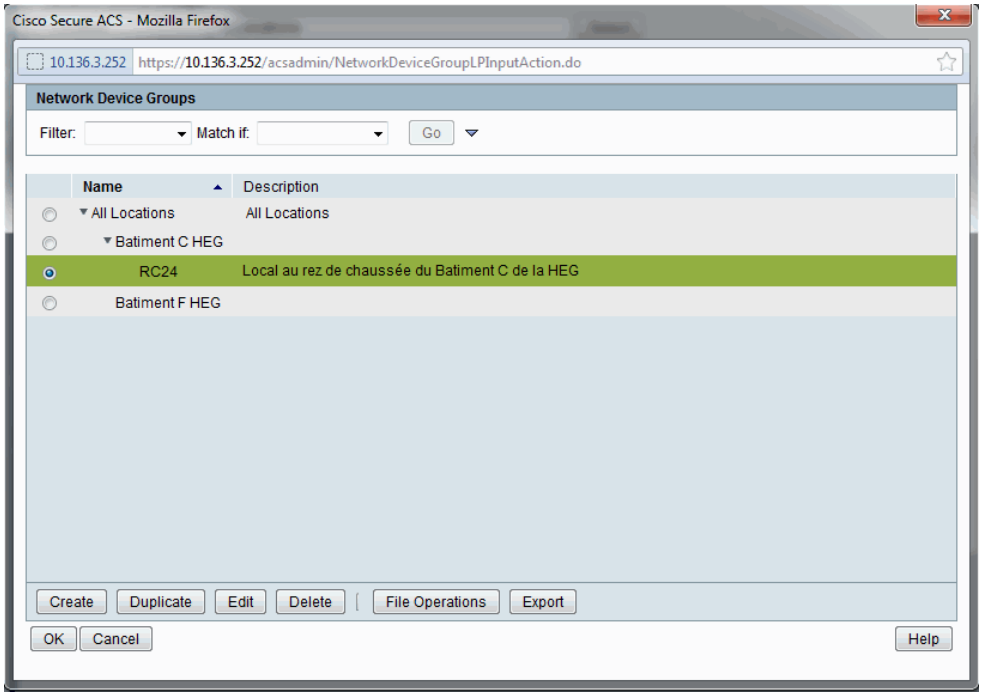

Figure 34: Création d'emplacements

Une fois les types d'équipements et d'emplacements définis, on peut créer l'entrée pour notre switch authentificateur, comme montré sur cette image.

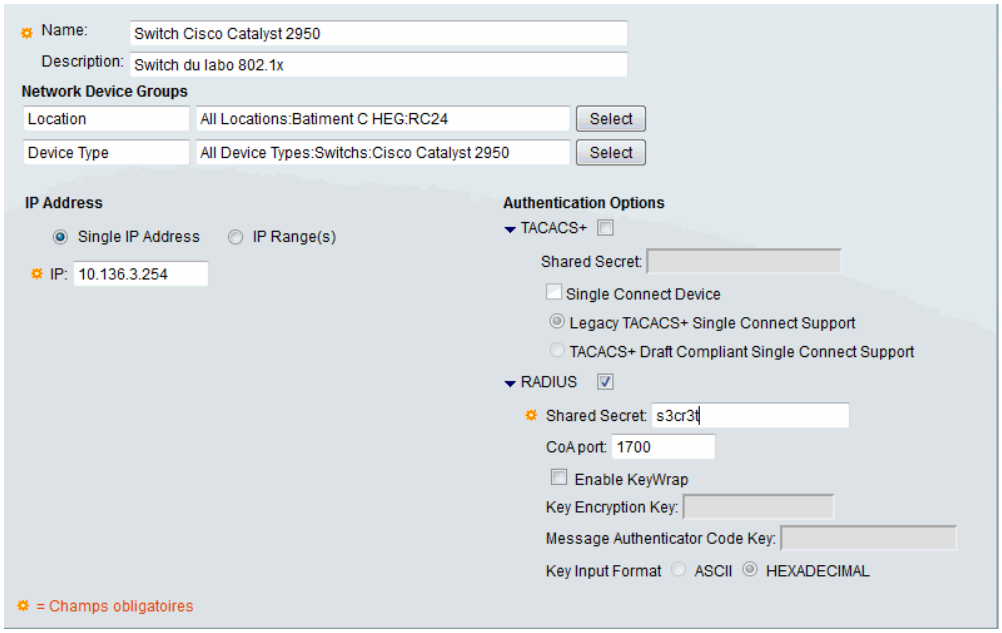

Figure 35: Enregistrement du switch

Nous spécifions donc un nom d'équipement, une description sommaire, suivi de l'emplacement de cet équipement et son type. On utilise pour cela tout ce que nous avons défini précédemment. Il faut ensuite indiquer l'IP du device, ainsi que le secret partagé, qui ici est s3cr3t. Nous pouvons ensuite enregistrer notre entrée.

3.2.1.2.5 Configurer les données d'identité

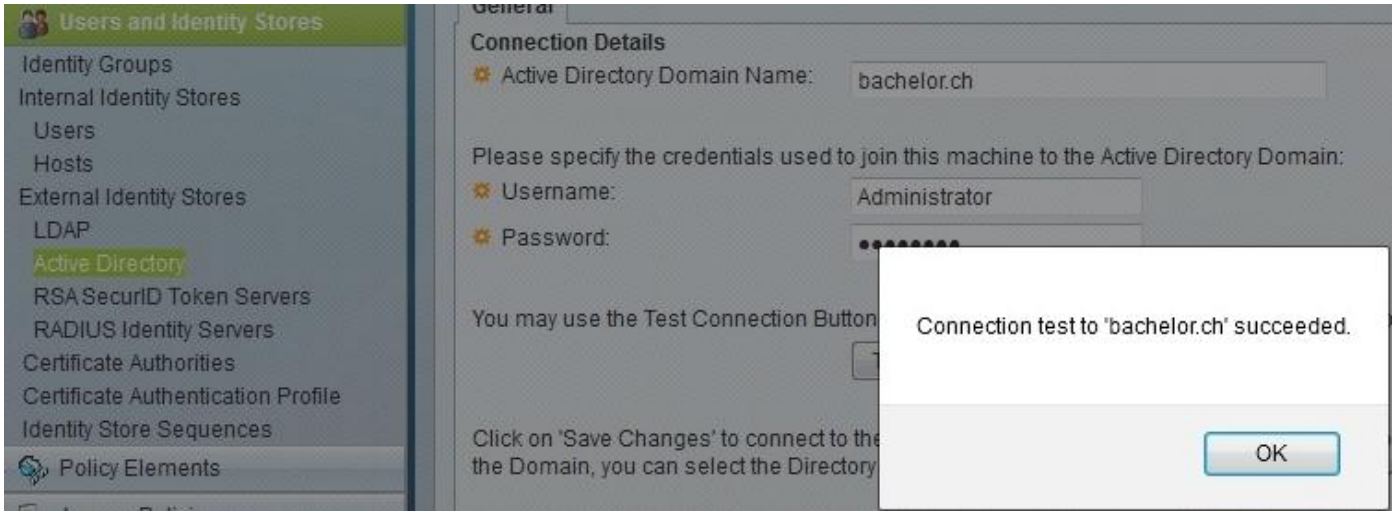

Figure 36: Connexion à Active Directory

Pour pouvoir utiliser une base d'utilisateurs externe, le moyen le plus pratique est le plus usité reste la base de données Active Directory. Nous connectons donc notre ACS au domaine avec un compte ayant les droits d'administrateur. Ceci nous permet de mettre en place la suite, qui est la sélection de la base d'utilisateurs.

3.2.1.2.6 Créer des règles d'accès

Nous utiliserons donc la base de données d'utilisateurs fournis par notre contrôleur de domaine pour authentifier les utilisateurs, puis nous appliquerons les règles d'accès spécifiques.

Figure 37: Sélection d'une base d'utilisateurs

Intéressons-nous au « Default Network Access » et plus précisement, aux protocoles que nous allons autoriser. La fenêtre correspondante se trouve à la page suivante du dossier.

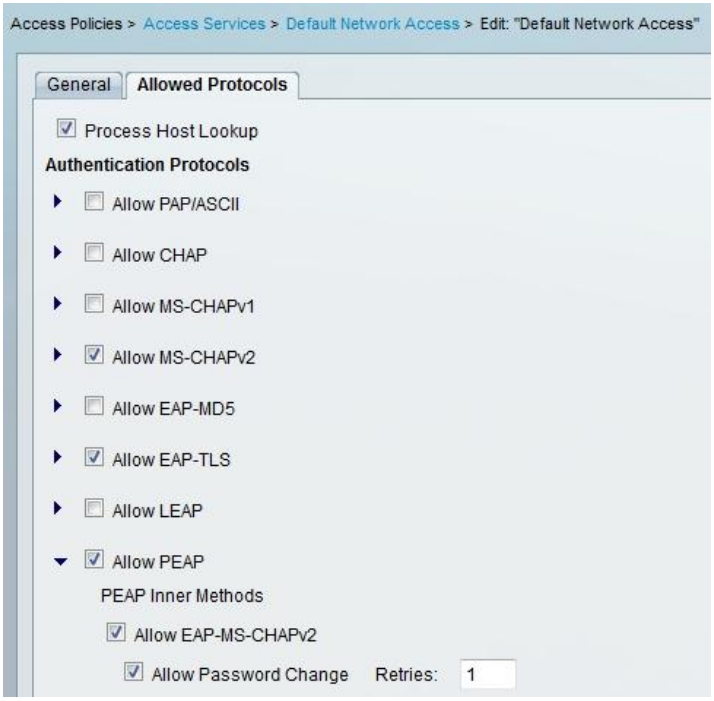

Figure 38: Protocoles autorisés

Nous observons qu'il nous faut cocher au minimum le protocole PEAP avec EAP-MS-CHAPv2. Nous avons également le choix d'utiliser des méthodes moins sécurisées ou au contraire plus sécurisées. Pour rappel, ces protocoles sont décrits au début de ce dossier.

C'est un paramétrage qui est général et qui s'appliquera à toutes les règles d'accès que nous créerons par la suite dans la section « Default Network Access ». Nous allons maintenant voir quelles étapes sont nécessaires pour mettre en place une règle d'accès.

La première nécessité, comme cela a été dit en introduction à propos de Cisco ACS, est de respecter le « si condition, alors profil d'autorisation ». Il nous faut donc définir une condition puis un profil d'autorisation que nous pourrons par la suite attribuer à une règle d'accès. Commençons par créer une condition régissant l'accès.

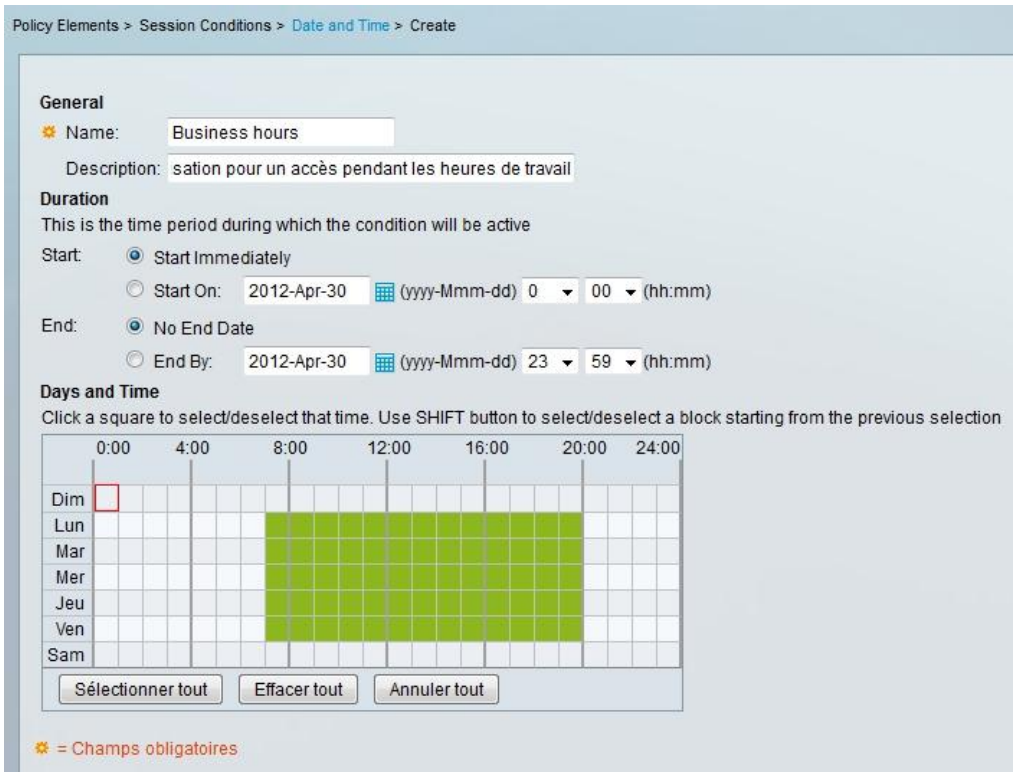

Figure 39: Business Hours

Comme vous pouvez le voir sur la figure précédente, nous n'allons autoriser l'accès au réseau que pendant les heures de travail et en semaine. Quel va ensuite être le résultat quand l'on répond ou non à cette condition ? Nous créons un nouveau profil d'autorisation. Figure suivante.

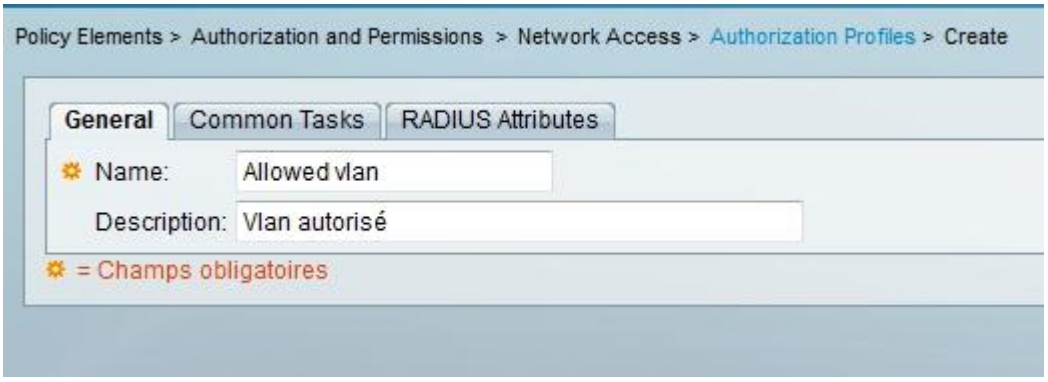

Figure 40: Profil d'autorisation

Ce profil sera celui d'un accès autorisé, nous pouvons définir directement les attributs RADIUS que nous voulons lui attribuer.

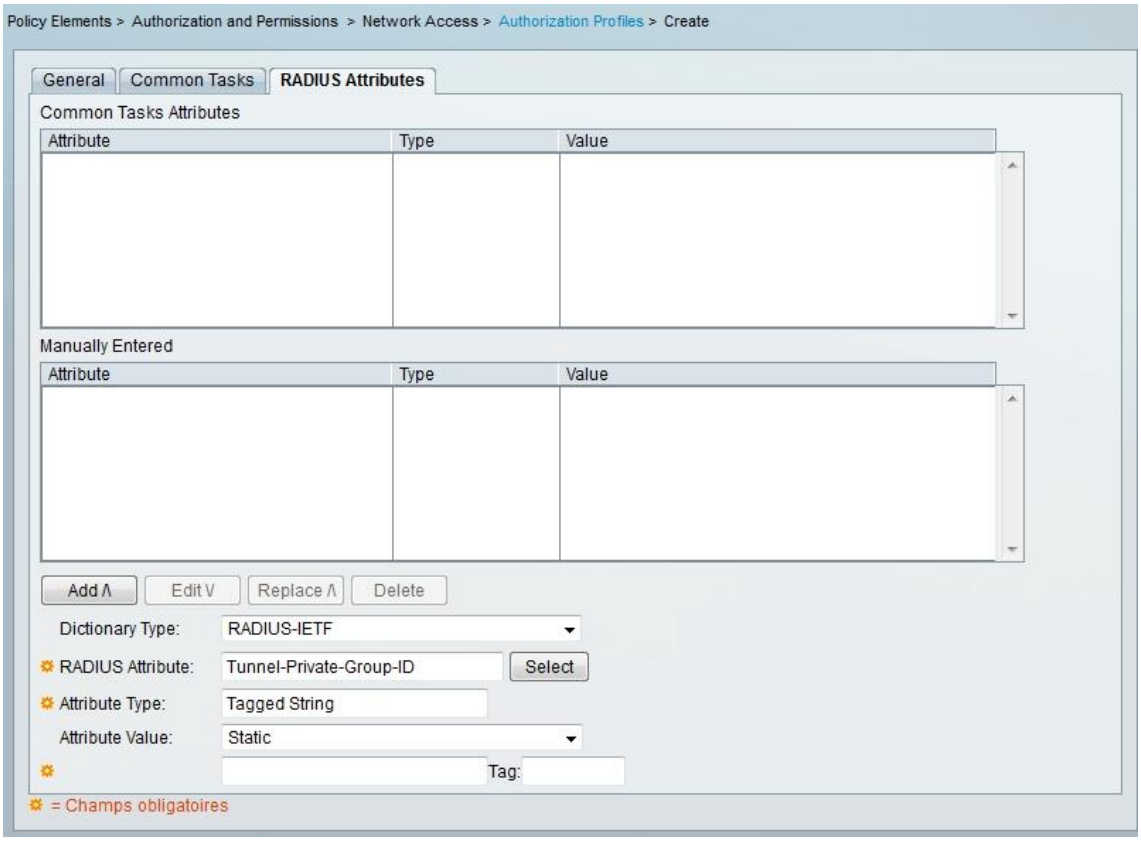

Figure 41: Attributs RADIUS

Ou plus simplement, dans les tâches habituelles (« Common Tasks »), l'on retrouve le fait d'attribuer un VLAN à ce profil d'autorisation, nous allons donc choisir cette option en configurant le VLAN statique numéro 3.

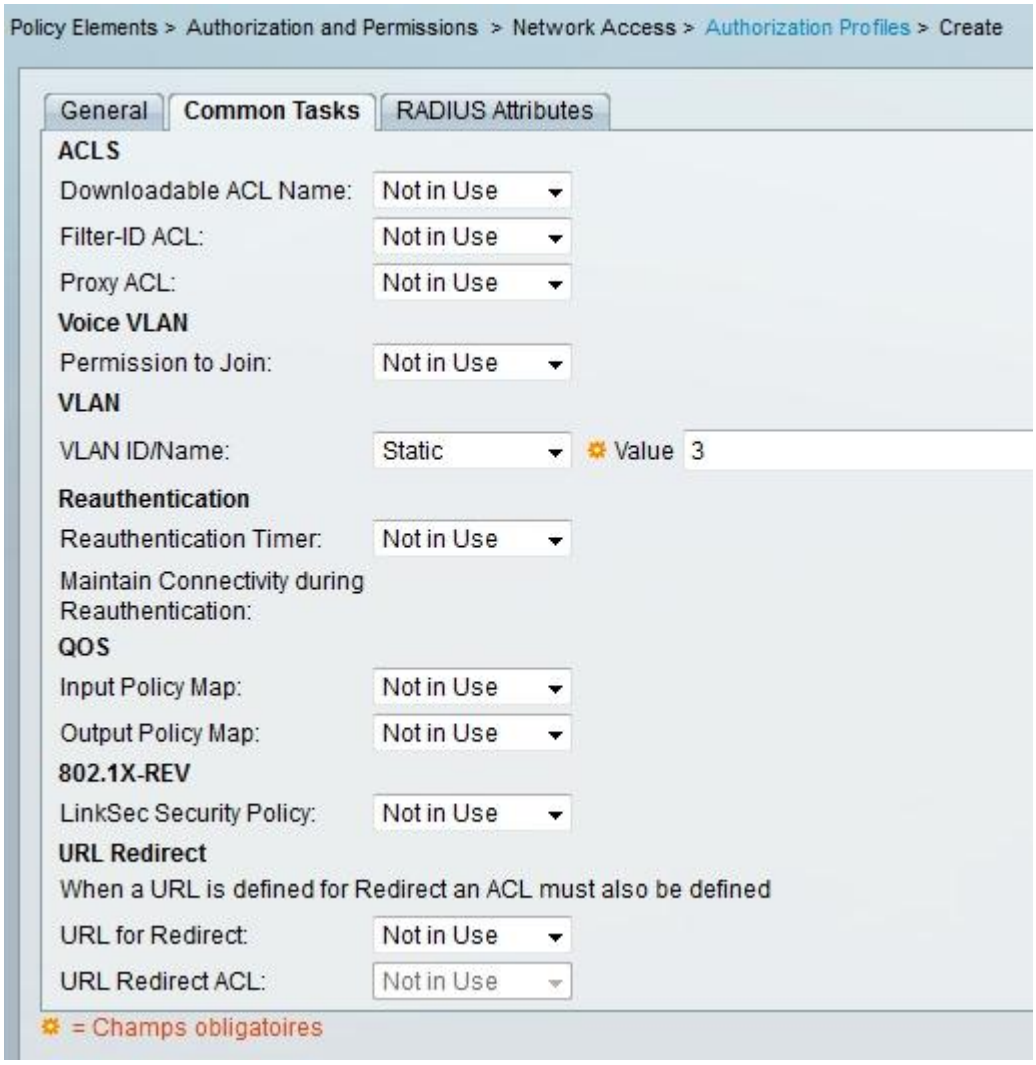

Figure 42: Common Tasks

Ce qui a pour effet de remplir automatiquement les champs RADIUS correspondants.

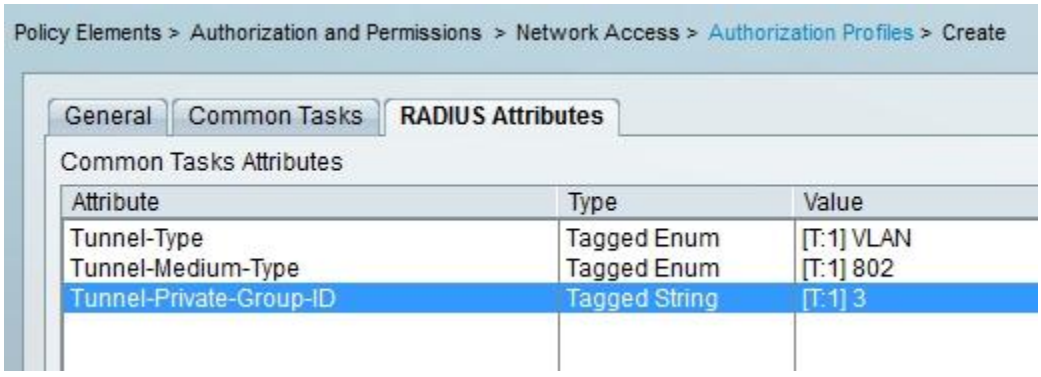

Figure 43: Configuration des attributs RADIUS automatique

Nous voyons clairement ici que les attributs utilisés lors de la configuration du labo Windows Server 2008 sont repris exactement de la même façon par Cisco ACS. Pour finir, nous créons un dernier profil d'autorisation pour le VLAN de quarantaine. Toutes les options seront identiques si ce n'est le numéro de VLAN, qui sera le 2.

Nous pouvons passer à la création des règles d'accès.

Standard Policy| Exception Policy

Network Access Authorization Policy

Filter: Status Match if: Equals Enabled Clear Filter Go

		Status	Name	Conditions			Results	Hit Count
				NDG:Location	Time And Date	AD1:ExternalGroups	Authorization Profiles	
1			CorporateAccess	in All Locations:Batiment C HEG:RC24	match Business hours	contains any (bachelor.ch/Users/IT Department)	Allowed vlan	0
2			NoBusinessHours	in All Locations:Batiment C HEG:RC24	does not match Business hours	contains any (bachelor.ch/Users/IT Department)	denied vlan	0

Figure 44: Règles d'accès

Nous avons donc deux règles d'accès, une qui répond à la condition des « Business Hours » et l'autre qui n'y répond pas. Un profil d'autorisation correspondant est ensuite attribué à chaque règle. Précisons ici que l'on peut utiliser des groupes Active Directory comme conditions pour les règles d'accès, ainsi que l'emplacement du client sur un de nos sites.

3.2.1.3 Résultat

Le résultat de ce laboratoire reste similaire au précédent, si l'heure et le jour de la tentative de connexion réponde aux exigences, le client aura un accès complet (Internet, ressources internes), si ce n'est pas le cas, il n'aura aucun accès. Il faut cependant penser au cas où le client se connecterait à 19h59 en mode autorisé. Comment lui enlever l'accès après 20h00 comme défini dans notre politique ? Cela ne peut se faire qu'à l'aide de la réauthentification périodique. La commande à rentrer sur le switch est la suivante :

```
# dot1x re-authentication
```

La période par défaut est de 3600 secondes, soit 1 heure. Bien sûr c'est beaucoup trop dans notre cas, nous allons modifier cette valeur à 2 minutes, soit 120 secondes. Pour cela, nous tapons :

```
# dot1x timeout re-authperiod 120
```

Nous voilà certain que le client ne dépassera pas de plus de deux minutes son temps imparti !

3.3 Open source

Quels sont les avantages d'une solution open source ? Ce n'est un secret pour personne, c'est gratuit. Sans compter qu'en plus d'être payantes, la plupart des solutions NAC valent leur pesant d'or[20]. Il ne faut cependant pas oublier que la plupart des produits OpenSource offrent un support commercial, qui est lui payant.

Pour donner un exemple, PacketFence offre 4 formules, à respectivement 550€ / 1'100€ / 3'750€ et 7'500€ par année de support. Pas extravagant, mais pas non plus gratuit au sens où on l'entend.

Voici les deux solutions NAC open source que j'ai trouvées lors de mes recherches :

- PacketFence
- FreeNAC

3.3.1 PacketFence

PacketFence ZEN (Zero Effort NAC) est fourni sous forme de machine virtuelle, qui nécessite plus ou moins d'efforts afin d'être adapté à l'environnement de travail. La compréhension de l'architecture est plutôt complexe, PacketFence étant un énorme outil à tout faire, plutôt qu'une solution orientée pour une utilisation précise. Pour ce travail j'ai dû renoncer à la VM préconfigurée, celle-ci étant tout sauf configurée pour mon type de labo. J'ai donc commencé par installer PacketFence comme un package sur une machine CentOS de base. J'ai eu quelques soucis à la mise en place du service MySQL mais au final j'ai pu accéder à l'interface graphique de PacketFence. Je me suis alors rendu compte que la configuration ne se fait pas du tout sur cette interface graphique. Tout est manuel dans les fichiers de configuration, ou alors il faut ajouter un freeradius avec tous les ennuis qui vont avec pour le connecter à un domaine Active Directory. J'avais déjà fait cette manipulation en labo école et refaire ce travail n'apporte pas de valeur à mon dossier. L'interface web permet donc, tout au plus, de gérer le produit en fonctionnement. Bien que la documentation soit bien fournie, elle est loin d'être claire pour le novice et le prix de son déploiement par un professionnel doit être envisagé, avec le coût que cela engendre. Je n'ai donc pas mis en œuvre de labo sur PacketFence, le manque d'exemples fonctionnels dans la

[20] Meilleur prix pour Cisco NAC Appliance neuf : $25,690

documentation et le temps qui m'était imparti en sont deux raisons. Ce produit est tout de même évalué selon l'expérience que j'ai eue.

3.3.2 FreeNAC

FreeNAC a été créé par Swisscom et est également un logiciel libre, qui fournit également une version commerciale. Le projet est cependant à l'arrêt depuis 2010. Il présentait une facilité apparente de déploiement, mais malheureusement il n'y avait pas de véritable valeur à tester un logiciel qui n'est à terme pas viable ni évolutif.

4. Comparaison des différentes solutions 802.1X

Pour pouvoir comparer efficacement les différentes solutions qui s'offrent à nous en termes de solutions pour implémenter le contrôle d'accès 802.1X, il nous faut définir des critères d'évaluation qui détermineront la valeur du produit.

L'échelle d'évaluation que je vais utiliser est la suivante :

- Très bon résultat – 5 points
- Bon résultat – 4 points
- Résultat moyen – 3 points
- Résultat faible – 2 points
- Résultat insuffisant – 1 point

Chaque point sera pondéré puis le total additionné donnera le score de chaque logiciel. Voici maintenant les critères évalués ainsi que leur pondération dans l'évaluation.

Prix de la solution - 25%

Le prix est un facteur primordial dans le choix d'une solution par une PME. Il est donc le critère ayant la plus forte pondération dans l'évaluation.

Qualité perçue du logiciel - 8%

La qualité du logiciel est évidemment un critère subjectif, mais dans notre cas il sera basé sur la simplicité d'utilisation perçue, la difficulté à surmonter les éventuels problèmes faisant obstacle à la mise en place, etc.

Réputation et position de l'entreprise qui produit le logiciel - 10%

La durabilité et la position sur le marché de l'informatique de l'entreprise qui produit la solution est importante. En effet, si l'entreprise périclite, il est évident que le support ne pourra plus être assuré. Il en va de même pour les mises à jour.

Support - 7%

Le support d'un produit

Documentation et exemples - 12%

La documentation est très importante. Non seulement elle permet de comprendre le fonctionnement du produit, mais elle permet aussi la résolution de problèmes sans forcément faire appel au support.

Facilité de mise en place - 10%

Ce critère correspond au temps nécessaire à une installation et à la complexité de cette dernière.

Suivi du produit - 8%

Ce critère évalue la fréquence des mises à jour et le suivi apporté au produit.

Intégration - 20%

Ce critère détermine si la solution s'intègre bien dans une infrastructure existante. C'est d'une importance capitale pour une société, si l'intégration n'est pas bien gérée, la solution n'a aucun intérêt.

	Windows Server 2008 R2	Cisco Secure ACS	PacketFence
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 Doc.	**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	**4.53**	**3.78**	**3.71**

4.1 Explication

4.1.1 Prix

Evidemment PacketFence est un logiciel gratuit, sa note est donc en conséquence. Windows Server 2008 R2 a un prix raisonnable, tandis que les logiciels Cisco sont un peu plus onéreux de manière générale.

4.1.2 Qualité

Ma notion de la qualité repose avant tout sur l'efficacité et la simplicité et l'ergonomie de l'interface graphique. Microsoft et Cisco s'en sortent avec une très bonne note, et l'opensource avec une bonne note également, mais pas à la hauteur des deux autres.

4.1.3 Solidité

La solidité de Microsoft sur le marché ne nécessite que très peu d'explications, la gamme Windows est la plus répandue et la plus achetée du marché en termes d'OS. Microsoft est un géant qui innove constamment, aucun risque donc que le produit ne disparaisse. Cisco est un géant lui aussi, mais à pieds d'argile. L'innovation se fait poussive et la virtualisation totale du réseau gagne des parts de marché ainsi que la concurrence asiatique. Cisco reste cependant le leader mondial en termes de parts de marché… pour le moment. Une note plutôt moyenne pour PacketFence, car l'opensource, prenant FreeNAC à titre d'exemple, peut s'arrêter d'un jour à l'autre. Par manque d'envie, de financement ou toute autre raison. La solidité d'une multinationale n'est clairement pas présente.

4.1.4 Support

Pourquoi donner une mauvaise note à Microsoft et Cisco ? Car en tant que simple utilisateur, il est impossible d'obtenir du support gratuit. Le prix pour obtenir du support est également exorbitant. Par chance, ils s'en sortent beaucoup mieux sur la documentation, ce qui permet de largement compenser. Le support open source est en général plus disponible, par le biais de forums d'utilisateurs par exemple.

4.1.5 Documentation

Nos deux premières solutions ont de la documentation sur Internet extrêmement fournie, sûrement du fait de leurs larges utilisations. Des exemples, des vidéos, tout y est. Quant à PacketFence, on ne peut pas en dire autant. La documentation est technique et précise, mais peu détaillée et absolument pas mis dans un contexte. Mauvaise note donc pour l'opensource.

4.1.6 Facilité d'utilisation

Ce critère découle du précédent, mais comprend également la clarté de l'interface de gestion. Les notes parlent d'elles-mêmes.

4.1.7 Suivi

Le suivi pour les produits propriétaires est bon, les mises à jour et les nouvelles versions sortent régulièrement. L'opensource obtient une meilleure note car les

releases sont généralement faites plus souvent et les bugs corrigés rapidement par la communauté.

4.1.8 Intégration

Les parcs informatiques étant en majorité sous Windows, l'intégration avec Windows Server et ses fonctionnalités se déroulent en général sans accro. Pour Cisco, bien sûr le lien au domaine AD peut se faire, mais il est loin d'être parfaitement implémenté. Je me suis retrouvé avec une liaison défaillante pour des raisons d'horloge, alors que l'heure était réglait exactement à la seconde prêt sur les deux machines. N'ayant pas pu évaluer correctement PacketFence sur ce point, il reçoit donc la moyenne.

4.2 Résultat

D'après mon évaluation, c'est donc Windows Server 2008 R2 qui s'en sort le mieux avec un score pondéré de 4.53 sur 5. Je recommande donc cette solution d'implémentation et je vous invite à lire ma conclusion à la page suivante.

Conclusion

Pour conclure ce dossier, je vais donner mon avis sur la solution que je trouve 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 toute entreprise qui souhaite se prémunir des dangers d'une machine dont l'état de santé est mauvais et potentiellement malveillant. Son prix reste raisonnable comparé aux couteuses implémentations d'autres grands constructeurs. Windows Server 2008 R2 a aussi l'avantage d'offrir de multiples fonctionnalités en plus, il fait en somme produit tout en un et c'est un avantage non négligeable.

Ce choix ne signifie pas que les autres solutions n'ont pas de mérite, au contraire, mais simplement qu'avec un budget raisonnable et un effort raisonnable on parvient rapidement à des résultats probants et efficaces. La compatibilité entre produits Microsoft n'y est évidemment pas pour rien.

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

Bibliographie

Littérature

BORDERES, Serge. *Authentification réseau avec Radius : 802.1x, EAP, FreeRadius*. Paris : Eyrolles, 2006. 209 p..

Web

802.1X et la sécurisation de l'accès au réseau local.
Luc Saccavini. Direction des Réseaux et Systèmes d'Information, INRIA
http://2003.jres.org/actes/paper.111.pdf

TECHNET. Support Microsoft Technet sur les technologies réseaux
http://technet.microsoft.com/en-us/network/

NETWORKWORLD. Ressources et articles sur tous les sujets réseaux
http://www.networkworld.com

WIKIPEDIA. Encyclopédie libre.
http://fr.wikipedia.org/

Examining 802.1x and EAP
http://ns1.netcraftsmen.net/welcher/papers/dot1x.pdf

Step By Step Guide: Demonstrate 802.1X NAP Enforcement in a Test Lab
http://www.microsoft.com/en-us/download/details.aspx?id=733

SolutionBase: Discover open source alternatives for NAC on your network
http://www.techrepublic.com/article/solutionbase-discover-open-source-alternatives-for-nac-on-your-network/178845

Annexe 1
Glossaire

Routeur

Un routeur est un périphérique réseau qui s'occupe de diriger le trafic de paquets sur un réseau IP. Il possède des chemins dans sa mémoire vive qui lui permettent de savoir où diriger quelle information et plusieurs interfaces réseaux pour recevoir ou envoyer les données. Il est en général utilisé pour faire le lien entre 2 réseaux IP(ou plus) différents.

Switch (commutateur)

Un switch est un périphérique réseau qui relie les différents équipements équipés d'interfaces réseaux entre eux. En général, il n'utilise pas les adresses IP mais seulement les adresses MAC pour acheminer le trafic. Un switch possède plus d'interfaces qu'un routeur, en général 24 ou 48 contre 1 à 5 pour ce dernier.

ESX

ESX est un hyperviseur, qui gère les ressources du système et les partage entre plusieurs instances de machine virtuelle tout comme Hyper-V de Microsoft. ESX Server est un produit de la société VMWare.

RADIUS

« Remote Authentication Dial-In User Service » est un protocole qui permet d'utiliser un ou plusieurs serveurs comme base centrales de données d'authentification, d'autorisation et de suivi des sessions utilisateurs.

TACACS+

« Terminal Access Controller Access-Control System Plus » est un protocole fournissant le même type de fonctionnalités que RADIUS avec des spécialités telles que l'attribution d'autorisation concernant les commandes IOS exécutables par un utilisateur sur un routeur ou un switch.

Annexe 2
Modèle OSI

Modèle OSI			
	Type de Donnée	Couche	Fonction
Couches Hôte	Donnée	7. Application	Point d'accès aux services réseaux
		6. Présentation	Gère l'encryptage et le décryptage des données, convertit les données machine en données exploitable par n'importe quelle autre machine
		5. Session	Communication Interhost, gère les sessions entre les différentes applications
	Segments	4. Transport	Connexions bout à bout, connectabilité et contrôle de flux
Couches Matérielles	Paquet/Datagramme	3. Réseau	Détermine le parcours des données et l'adressage logique
	Trame	2. Liaison	Adressage physique
	Bit	1. Physique	Transmission des signaux sous forme binaire