Quarantaine et remédiation - Réalisation et utilité

Richard Timsit, Daniel Grandjean

Quarantaine et remédiation

Réalisation et utilité

Richard Timsit
École Polytechnique Fédérale de Lausanne (Service téléinformatique DIT-TI)
Ecublens Lausanne Suisse
Richard.Timsit@epfl.ch

Daniel Grandjean
École Polytechnique Fédérale de Lausanne (Service téléinformatique DIT-TI)
Ecublens Lausanne Suisse
Daniel.Grandjean@epfl.ch

Résumé

Dans un campus où le nombre de postes de travail raccordés à Internet dépasse celui des étudiants et du personnel (plus de 10000), veiller à la sécurité des ressources informatiques à disposition est une gageure. Ne voulant pas rester impuissants face aux grandes vagues d'infection des machines Windows dans le début des années 2000, nous avons conçu et déployé un réseau de quarantaine. Nous décrivons ici le système mis en place et le bilan que nous tirons de son utilisation. Forts de cette expérience et profitant d'une partie de l'infrastructure existante, nous avons mis en place un réseau de remédiation que nous décrivons pareillement.

Mots clefs

Virus, quarantaine, remédiation, sécurité

1 Introduction

L'EPFL est un grand campus situé en Suisse au bord du Léman. Comme il n'est pas de territoire neutre dans le cyberespace, en 2003 nous n'avons pas été épargnés par le virus Sasser.A et nous nous sommes posé les mêmes questions que partout ailleurs : à quel niveau couper la machine du réseau ?

- soit nous isolons sa prise de raccordement au réseau et nous privons son utilisateur de toute information et de tous les outils pour réparer son poste de travail ;
- soit nous lui coupons seulement l'accès à Internet en la laissant polluer l'Intranet.

Pour éviter ce dilemme stupide, nous avons conçu un réseau de quarantaine. Ensuite, pour satisfaire les demandes d'utilisation de ce réseau à des fins préventives, nous avons construit un réseau de remédiation sur le réseau libre-service (réseau d'amarrage) du campus.

2 Cahier des charges

Nous voulions que la détection de l'infection d'une machine permette :

- d'isoler immédiatement la machine de notre réseau (EPNET) tout en lui laissant l'accès à un certain nombre de services utiles ;
- d'informer l'utilisateur (ou l'administrateur du poste de travail) de la situation dans laquelle la machine se trouvait :
  - par un courriel aux différentes personnes susceptibles de gérer cette machine (assez aléatoire) ;
  - par la page d'information que le butineur de l'utilisateur récolterait à la moindre tentative d'accéder à une URL (proxy web transparent) ;
- de donner les moyens de patcher, nettoyer et supprimer les failles de sécurité pour prévenir d'autres infections ;
- de permettre à l'utilisateur de sortir son poste de travail de quarantaine automatiquement au moyen d'un formulaire web.

3 Contexte

Un campus d'environ 250000 m² construit à la fin des années 1970, en perpétuelle extension, fait l'objet d'un câblage systématique depuis 1992. Des câbles de catégorie 5, 5E, 6 puis 6A rayonnent dans tous les locaux du campus à partir d'une centaine de locaux de brassage où sont situés nos équipements actifs. Plus de 40000 prises sont installées, dont 20000 sont raccordées sur des ports de commutateurs administrables. Nous nous sommes donnés les moyens de gérer notre câblage afin de savoir dans quel local se trouve chaque prise ethernet et de disposer de leurs coordonnées GIS [1] ce qui permet leur visualisation sur des plans. Nous essayons de faire en sorte qu'une seule machine soit raccordée sur chaque prise, les micro-commutateurs disposés dans un local n'étant qu'exception.

Quelques 400 points d'accès Wi-Fi sont venus offrir de nouvelles façons de se connecter au réseau pour répondre à

de nouveaux besoins de nomadisme, ce qui pose aussi de nouveaux problèmes de sécurité.

Disposant de deux plages d'adresses de classe B et de quelques agrégats de classe C, nous faisons partie des nantis de ce point de vue et n'adopterons pas IPv6 pour une raison de carence en adresses IPv4. Cet atout nous permet de faire du *subnetting* et nous a donné un grand confort pour segmenter notre réseau avant de disposer de Vlan.

La distribution en Vlan épouse la structure administrative qui est aussi topographique (bâtiments, facultés, instituts) ce qui nous évite d'avoir à les étendre inutilement.

Notre architecture ressemble à beaucoup d'autres aujourd'hui... La course au débit faisant place à un besoin grandissant de fiabilité, vous observez beaucoup de redondance sur la figure 1. La plupart des liaisons sont des liens à 1Gbs ; quelques liens à 10 Gbs commencent à être installés entre le Catalyst du centre 1 et les Catalysts de distribution de facultés.

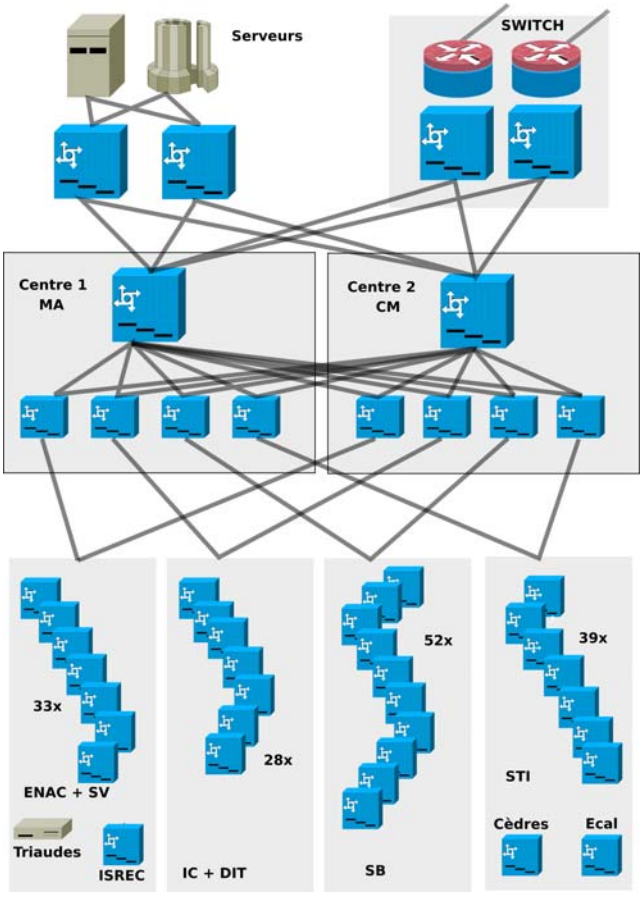

Figure 1 – Schéma du réseau EPNET

Nous disposons entre EPNET et Internet (SWITCH) [2] d'un système baptisé DIODE [3] fonctionnant comme un firewall sans grandes contraintes. Nous ne voulions pas donner l'impression que les machines du campus étaient derrière un mur de protection. Ce qui ne se voit pas sur le schéma c'est que l'accès au réseau du campus par VPN est tout aussi possible que le raccordement d'une machine nomade sur le réseau de son laboratoire avec ou sans câble...

4 La mise en quarantaine

Mettre en quarantaine une machine connectée sur le réseau câblé, c'est faire basculer le port du commutateur sur lequel elle est raccordée dans un Vlan spécial, le Vlan de quarantaine. Sur ce Vlan est raccordé l'automate qui va gérer les machines tombées en quarantaine, offrir les services nécessaires à leur maintien en vie sur le réseau et acheminer sur l'Intranet et sur Internet les flux de communication nécessaires à leur réparation.

Pour les clients associés par WPA sur le Wi-Fi du campus, la mise en quarantaine est aussi possible. Un Vlan est prévu à cet effet et au moment de l'authentification de l'utilisateur dont la MAC adresse a été repérée, le serveur RADIUS peut forcer le point d'accès à utiliser ce Vlan pour ce client. Les services de quarantaine sont alors rendus comme sur le câble. Nous n'avons cependant pas déployé cette solution qui réclame une gestion lourde du serveur RADIUS et traitons ces nomades comme ceux qui passent par un concentrateur VPN : nous les informons par courriel de l'infection de la machine avec laquelle ils se sont connectés.

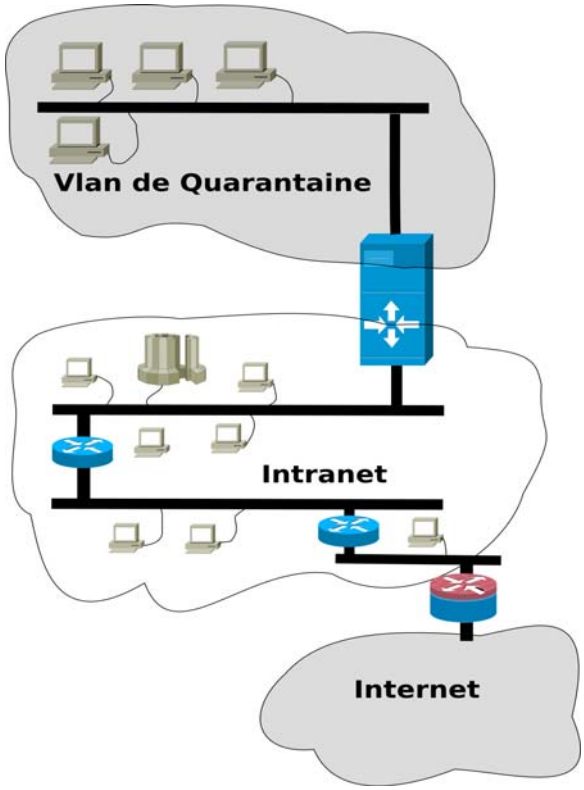

Figure 2 – Principe de la quarantaine

4.1 Les services à assurer

En quarantaine, les services assurés sont réduits au minimum, mais suffisants pour que le poste de travail reste utilisable sur le réseau.

4.1.1 DNS

Afin que la résolution nom-adresse puisse continuer à se faire, un service doit être rendu dans les mêmes conditions que sur le réseau du campus.

4.1.2 DHCP

De même, si l'adresse IP de la machine tombée en quarantaine avait été distribuée par un serveur DHCP, il faudra en quarantaine continuer à la lui donner.

4.1.3 Routeur par défaut

La machine gardera tous ses paramètres réseau et devra donc continuer à disposer du service de son routeur par défaut.

4.1.4 Un proxy transparent pour le web

Comme l'utilisateur continue à travailler sur sa machine alors qu'elle a glissé d'un réseau sur un autre, il faut bien l'avertir de ce qui lui arrive. Le proxy transparent est ce que nous avons trouvé de mieux pour l'avertir rapidement et indiquer la conduite à tenir.

Toute tentative d'accéder à une ressource du web donnera une page explicative et proposera les liens à suivre pour disposer des informations et permettre la réparation. Cependant, toute URL utile pour se documenter ou patcher sa machine restera accessible.

4.1.5 Le maintien du contact avec l'agent antivirus

Chaque machine Windows sur le campus héberge un agent ePO de McAfee qui permet autant la collecte des événements d'infection et d'intrusion que l'installation, la configuration et la mise à jour des produits de protection comme l'antivirus, l'anti-spyware et l'IPS software.

La communication entre les agents et le serveur ePO doit être maintenue pour pouvoir contrôler l'état d'alerte et de mise à jour des produits de protection installés. Ajouter des produits manquants, déployer des signatures spécifiques ou appliquer une contre-mesure peut constituer une aide précieuse pour permettre le nettoyage du PC tombé en quarantaine.

4.1.6 La possibilité d'accéder aux sites de Microsoft pour réaliser la mise à jour Windows Update...

Ce service n'est pas facile à offrir à cause des techniques utilisées par Microsoft, mais nous pouvons quand même le rendre efficacement sans ouvrir le réseau de façon aveugle à l'HTTPS.

4.1.7 La possibilité d'accéder à différents serveurs de logiciels.

Comme les machines Windows n'ont pas l'apanage des virus et des vers, il est primordial de concevoir cet outil en considérant toutes les architectures utilisées sur le campus. Les principaux dépôts de logiciels doivent être accessibles du réseau de quarantaine ou du réseau de remédiation.

4.2 Comment utiliser un tel système ?

L'activité réseau des machines infectées par des vers étant encore détectable (la situation a changé ces dernières années, les vers sont devenus plus furtifs et leur mode de propagation s'est transformé à l'exemple de la famille SdBot), on ne manque pas totalement de moyens pour être alerté, voire pour déclencher une mise en quarantaine de façon automatique. Nous avons commencé par utiliser une sonde **Snort,** puis les informations remontées par les agents installés sur les PC et enfin nous bénéficions des alertes que notre fournisseur d'accès Internet SWITCH nous communique. La majorité des mises en quarantaine aujourd'hui se fait manuellement.

Les premières informations dont on dispose sont l'adresse IP de la machine infectée et l'heure à laquelle cette détection a eu lieu. À partir de l'adresse IP, il faut disposer de la MAC adresse qui lui était associée à ce moment-là et du port sur lequel elle a été vue. Sur le réseau câblé, cette chaîne est assez facile à suivre pour peu que l'on ait un matériel confortablement administrable et que l'on se soit construit les bons outils (une panoplie de scripts écrits en Perl). Pour les accès Wi-Fi au réseau, il faut pouvoir agir au moment de l'authentification ou de la réauthentification et forcer le Vlan du client associé.

4.3 Quelle architecture adopter ?

4.3.1 Deux en une

Nous avons choisi d'utiliser deux machines dont l'une sur le réseau de quarantaine voit toutes les machines dans ce Vlan comme étant sur son réseau de classe B. Elle communique avec une autre machine de notre réseau à travers un réseau privé de communication réservé à ces deux machines. Une machine physique avec plusieurs interfaces Ethernet tournant un OS permettant d'accueillir une machine virtuelle est la solution optimale. Nous avons utilisé UML [4] quand nous avons démarré le projet ; un grand choix de systèmes de virtualisation ou de paravirtualisation permettrait aujourd'hui de construire facilement la solution.

4.3.2 Les briques de base

Les noyaux des machines GNU-Linux et les distributions courantes nous offrent tout ce qu'il faut pour réaliser notre dispositif:

- un firewall ;
- des bridges logiciels [5];
- des serveurs pour les services DNS et DHCP.

Les applications spécifiques tournent autour d'un serveur Apache et d'un proxy ou d'un module proxy. Nous avons choisi **Squid** [6] couplé avec **Jesred** [7] pour la redirection.

4.4 Dans le ventre de l'automate

Le but de cet article n'est pas d'entrer dans les détails d'une implémentation qui dépend intimement de l'infrastructure déployée, mais d'en donner les grands principes qui

pourraient être utilisés et adaptés à toute configuration de campus. Commençons par une machine avec 2 interfaces réseau, l'une raccordée sur **EPNET** et l'autre raccordée sur le réseau de quarantaine que l'on nommera **EPNAZ**.

4.4.1 Configuration de la machine sur le réseau EPNAZ

C'est une machine virtuelle instanciée sur la machine physique de la façon la plus rustique qui soit. Elle n'a rien besoin d'autre que de disposer de deux interfaces réseau, l'une sur le réseau de quarantaine pour servir ses clients et l'autre pour dialoguer avec le serveur connecté au reste du monde.

La liaison entre les deux interfaces réseau est filtrée par le firewall IPTables. Celui-ci interdit tout trafic sauf HTTP et HTTPS. Les flux HTTP sont redirigés de manière transparente vers le proxy Squid hébergé sur la deuxième machine connectée au réseau EPNET. Le proxy ne permet l'accès qu'aux URL nécessaires à la réparation du poste. Les flux HTTPS ne sont quant à eux autorisés qu'à destination des serveurs Windows Update et d'authentification pour la sortie de quarantaine.

Les services déjà énumérés, que nous allons devoir rendre, obligent une configuration judicieuse de l'interface sur le réseau de quarantaine avec le bon netmask pour pouvoir empiler toutes les adresses nécessaires : celles du DNS et du routeur par défaut pour chaque subnet concerné par une machine introduite dans ce réseau.

La configuration du DHCP est modifiée pour prendre en charge tout nouvel arrivant et quelques fichiers sont mis à jour pour que des pages dynamiques web lui soient proposées.

4.4.2 Configuration de la machine sur le réseau EPNET

C'est elle qui va faire l'acheminement et le contrôle de tous les flux entre les machines en quarantaine et EPNET/Internet.

Le tandem **Squid-Jesred** joue un rôle classique de filtre des URL et de redirection.

Pour que le **Windows Update** fonctionne, on doit ouvrir l'accès pour l'HTTPS vers des adresses IP dont la résolution ne donne pas toujours une réponse, aussi faut-il de temps en temps réactualiser une liste de réseaux utilisés par Microsoft pour cette fonction et paramétrer le firewall en conséquence.

Cette machine étant accessible du réseau EPNET, c'est par elle que se fait toute la gestion des machines en quarantaine et par elle que passe tout le contrôle des clients de ce service comme celui de la remédiation.

4.5 Quels services cela rend-il ?

4.5.1 Soustraction immédiate des machines infectées

Lorsque l'infection d'une machine est détectée, cette dernière est mise en quarantaine de manière automatique ou manuelle. Il en résulte un isolement immédiat de la source de propagation d'attaque. L'efficacité et la rapidité de cette mise en quarantaine évitent la propagation d'une infection à large échelle sur notre parc de machines. Dans le cas d'une infection via une faille largement répandue et non-corrigée, cet outil participe radicalement au confinement du problème et améliore d'autant sa résolution.

4.5.2 Meilleure information des utilisateurs

Les utilisateurs sont souvent pris au dépourvu lorsqu'ils sont confrontés à une problématique de sécurité touchant leur ordinateur. Leur comportement peut paraître irresponsable, ignorant les avertissements et se contentant de continuer à travailler loin des préoccupations de sécurité inhérente à leur machine. Ils peuvent, à l'inverse, être paniqués, cherchant des informations ou de l'aide pour résoudre ce qu'ils considèrent comme une action nécessaire, mais irréalisable à cause de leur connaissance réduite vis-à-vis de ce problème.

La mise en quarantaine s'accompagne d'une information précise sur les raisons de l'isolement de leur machine. Elle permet donc à l'utilisateur de comprendre pourquoi l'accès au réseau lui a été momentanément retiré et évite une perte de temps et de nombreux coups de téléphone.

Elle donne également accès aux différentes procédures à suivre en cas d'infection et aux conseils pour assurer un niveau de sécurité minimum. L'utilisateur peut télécharger via ce portail les divers outils pour patcher, protéger et nettoyer son ordinateur.

En cela, cette mesure est alors prise comme une aide et une protection plutôt que comme une punition.

4.5.3 Assainissement du parc des PC Windows

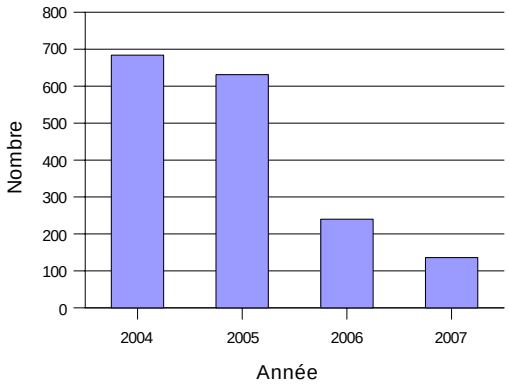

Figure 3 – Nombre de machines tombées en quarantaine

Depuis sa mise en place, le réseau de quarantaine a permis d'assainir le parc de machines qui, jusque-là, comptait un certain nombre d'ordinateurs régulièrement victimes d'attaques. La qualité de l'information fournie ainsi que l'adéquation des outils proposés a eu comme résultat une baisse constante des cas d'infection massive et les incidents

de ce type se résument aujourd'hui à un petit nombre de machines détectées quasi incompressible.

L'étude permanente des moyens mis à disposition depuis le réseau de quarantaine garantit l'efficacité de celui-ci et diminue donc d'autant les ressources nécessaires pour la prise en charge des appels. Le cas échéant, cela évite une longue intervention de nettoyage.

Il faut donc continuellement s'assurer que les utilisateurs ont pu, grâce aux informations et aux moyens mis à leur disposition, nettoyer leur machine de toute trace d'infection et empêcher l'éventuelle réinfection de celle-ci. Le formulaire de demande de remise sur le réseau universitaire remplit ce rôle important.

Nous constatons une augmentation régulière du nombre d'agents antivirus installés sur les machines (4500 en 2004 et 6000 aujourd'hui). La prise en charge des postes infectés dans le réseau de quarantaine et l'aide fournie aux utilisateurs dans ce contexte sont bénéfiques pour tout le monde. Les utilisateurs prennent conscience des enjeux de la sécurité et notre parc d'ordinateurs s'assainit.

5 La remédiation

La quarantaine en production, des utilisateurs et des administrateurs de systèmes ont souhaité disposer d'une ou plusieurs « prises Ethernet en quarantaine » stratégiquement situées ou d'un moyen d'entrer « volontairement » en quarantaine. Expérience faite, la quarantaine représentait pour eux un espace (cocon) protégé pour mettre à jour ou installer une nouvelle machine sans craindre qu'une application malveillante profite de cette fenêtre de vulnérabilité.

Ne souhaitant pas créer et gérer des prises avec un traitement particulier, nous avons choisi d'adapter une infrastructure existante, notre réseau d'amarrage.

5.1 Le réseau d'amarrage

Notre réseau sans fil Wi-Fi publie trois SSID. Chacun correspond à une technologie de contrôle d'accès :

- **epfl** - réseau protégé par WPA. Les services et l'adressage vont dépendre de l'authentification et de l'autorisation de l'utilisateur ;
- **MOBILE-EAPSIM** - protégé par WEP et 802.1x basé sur les cartes SIM de Swisscom. « L'opérateur historique » y fournit ses services à sa clientèle ;
- **public-epfl** - réseau Wi-Fi ouvert. Il offre les services de DNS et DHCP dans une plage d'adresses non routables et ne nécessite aucune configuration du client.

Le réseau **public-epfl** est notre réseau d'amarrage. Il est aussi largement accessible par plus de 1000 prises Ethernet RJ45 dispersées sur le campus et reconnaissables à leur couleur jaune. Il fournit une connectivité réseau de base en libre service. Le trafic entre les clients du réseau d'amarrage est volontairement restreint pour les protéger des comportements hostiles de voisins. En outre, ce filtrage empêche l'apparition sur ce réseau de services officieux ou usurpés et son utilisation abusive comme transport au travers ou entre nos sites.

Une fois connecté au réseau d'amarrage, différents **services** (accessibles via un portail captif) permettent au trafic d'en sortir, ceux-ci répondant aux besoins de plusieurs **populations** :

- service **VPN** - Les **étudiants** et le **personnel** utilisent nos concentrateurs VPN. Les membres d'autres institutions académiques avec lesquelles nous avons un accord d'échange de trafic se connectent librement à leurs concentrateurs VPN distants ;
- service **EnClair** [8] - Les **visiteurs** ou participants à une conférence qui ont été parrainés par leur hôte local peuvent ainsi accéder à Internet ;
- service **PWLAN** - Les **clients** des opérateurs de HotSpots commerciaux avec lesquels nous avons un accord d'échange de trafic sélectionnent le portail de leur opérateur. Notre réseau d'amarrage est considéré comme un HotSpot.

Et pour satisfaire la nouvelle demande de « quarantaine volontaire », le réseau de remédiation va profiter de l'omniprésence du réseau d'amarrage :

- service **SafeNetwork** - Les **utilisateurs** ou les **administrateurs** qui souhaitent un environnement protégé pour installer ou mettre à jour une machine choisissent le réseau de quarantaine.

5.2 Amarrage mis en œuvre

Le trafic du réseau d'amarrage est géré par une évolution du système *Multi Provider Portal*, MPP [9]. Le MPP a vu le jour pour faire cohabiter les fournisseurs d'accès Internet sans fil à l'aéroport de Zurich Kloten. Il fut ensuite adopté par plusieurs campus helvétiques dans le cadre du projet SWITCHmobile [10]. Le MPP est bâti avec les logiciels libres LAMP et netfilter.

Dans notre configuration, la haute disponibilité du service est assurée par le dédoublement du matériel et l'utilisation du protocole VRRP côté GNU-Linux et de HSRP avec tracking coté Cisco-IOS. Les flux spécifiques et internes au campus (DNS, VPN, HTTPS, IMAPS, SMTPS, SSH) sont routés directement. Tout le trafic du réseau d'amarrage restant est adressé au MPP. Il assure les fonctions de serveur DHCP, de portail web captif et de filtrage réseau.

5.2.1 Principe de fonctionnement

La tâche du MPP est d'appliquer pour la durée d'une session un routage dépendant de l'adresse d'origine du trafic. Chaque stratégie de routage est décrite dans un profil. Un profil est une collection de règles portant sur les adresses IP, les ports et les protocoles qui est compilée en commandes IPTables.

5.2.2 Condition initiale

Une session débute par l'attribution d'une adresse par le serveur DHCP. Le trafic en provenance de cette adresse est pris en charge tant que son bail est reconduit. À ce stade la

perméabilité du MPP correspond au profil par défaut. Ce profil définit les destinations accessibles inconditionnellement tels les concentrateurs VPN de partenaires ou les pages de services publics. Ces destinations sont appelées *open garden*. Dans notre configuration les adresses sources de tous ces trafics sont traduites en une seule adresse routable (PAT). Seuls les trafics HTTP et HTTPS restants sont redirigés vers le serveur Apache du MPP, les autres sont simplement ignorés.

5.2.3 Sélection explicite

L'utilisateur tentant de butiner à l'extérieur d'un *open garden* recevra une redirection temporaire (307) vers la *landing page* du portail d'accès. Sur cette page il peut sélectionner le lien du service de son choix ou remplir un formulaire de *login* pour accéder à des ressources qui nécessitent une authentification. Le choix du service va entraîner la sélection d'un profil de routage et induire un ordre de redirection pour le butineur. Cette dernière opération force le rafraîchissement de la page en empruntant la toute nouvelle route. On notera que cette approche permet de cascader plusieurs portails captifs. C'est un cas de figure courant des HotSpots commerciaux.

5.2.4 Sélection implicite

Un profil de routage peut être silencieusement assigné en fonction du HTTP-USER-AGENT initiateur du trafic. Cette particularité permet de satisfaire les attentes de certaines solutions de réseaux virtuels tels que iPass [11]. Elle permet aussi de traiter le trafic d'agents de mises à jour de certaines applications.

5.2.5 Services Authentifiés

Lorsque l'accès à un service est subordonné à authentification et autorisation, ces tâches sont déléguées à notre serveur RADIUS. C'est le cas de figure du service EnClair. Le trafic est traduit (NAT) dans une plage d'adresses routables considérée comme externe à notre périmètre de sécurité.

Dans sa version originale, le MPP ne supportait qu'un seul profil par formulaire de *login*. Pour étendre notre concept de quarantaine à tous les modes d'accès de notre réseau, nous avons spécifié quelques améliorations:

- la MAC adresse du client est communiquée au serveur RADIUS ;
- le serveur RADIUS retourne dans sa réponse le numéro du profil qui sera appliqué au client.

Nous disposons ainsi de toutes les primitives pour implémenter des procédures d'autorisations très fines. Mais à ce jour, ce n'est pas encore réalisé.

5.2.6 SafeNetwork

Pour le réseau de remédiation, connu comme le service SafeNetwork, nous avons créé un nouveau formulaire de *login* dans le portail captif. Le profil de routage modifie le *next hop* du trafic avec pour valeur l'adresse d'une interface supplémentaire ajoutée à la machine de quarantaine. Sa configuration est extrêmement simple et totalement statique. Il est inutile d'avoir une frontale virtuelle comme pour EPNAZ. DNS, DHCP, routage et authentification étant fournis par ailleurs, seuls sont requis les services de proxy transparent et de PAT pour un ensemble prédéterminé d'adresses non routables. Le partage de cette ressource entre la quarantaine et la remédiation centralise la maintenance des règles du proxy et donc celle des services disponibles dans ces 2 mondes.

5.2.7 Sortie de remédiation

Contrairement à la sortie de quarantaine où l'utilisateur est prié de s'authentifier et peut commenter son expérience, la procédure de sortie de SafeNetwork est directe. C'est un simple lien vers un CGI du portail captif qui rétablit le profil de routage par défaut.

6 Conclusion

Nous n'avons pas voulu attendre l'arrivée sans cesse repoussée d'un réseau capable de se défendre tout seul (Network Access Control de Cisco ou encore Unified Access Control de Juniper). La volonté de conserver la connectivité des machines que nous excluions dans le passé nous a conduits à construire le réseau de quarantaine.

Pour l'utilisateur, disposer d'une connexion réseau alors que sa machine est infectée par un ver ou un virus s'est avéré extrêmement pratique et confortable.

Pour les responsables de la sécurité, avoir la faculté de soustraire une machine du réseau tout en gardant le contact avec son utilisateur s'est avérée tout aussi utile.

Pour les gestionnaires du réseau que nous sommes, continuer à fournir un service sans mettre en péril l'infrastructure, procure une satisfaction certaine.

Forts de cette expérience, nous nous sommes adaptés à l'empilement des réseaux aux fonctionnalités spécifiques. Nous devons aujourd'hui nous forger les outils qui préservent l'illusion à l'utilisateur de disposer d'un unique réseau performant, fiable et sûr.

Nous vous proposons sur notre site [12] des informations complémentaires sur notre architecture.

Bibliographie

[1] http://plan.epfl.ch/index.html?js_folder_idx=5&view=277&view_text=jres

[2] SWITCH, réseau académique suisse, http://www.switch.ch/

[3] Projet DIODE, janvier 2000, http://ditwww.epfl.ch/SIC/diode/

[4] http://user-mode-linux.sourceforge.net

[5] http://linux-net.osdl.org/index.php/Bridge

[6] http://www.squid-cache.org/

[7] http://www.linofee.org/~jel/webtools/jesred/

[8] Réseau d'amarrage de l'EPFL,http://network.epfl.ch/EnClair/index.fr.html

[9] http://www.wlan-partner.com/hotspot-loesungen/wlan-access-portal/

[10] Projet SWITCHmobile, http://www.switch.ch/fr/mobile/

[11] http://www.ipass.com

[12] http://network.epfl.ch/JRES2007