DMZ décentralisée et VPN IPSec pour la connexion des UMR

Pierre Catala
INRA – DISI – Pôle Systèmes Informatiques – Service Infrastructure et Réseaux
UCIJ – 78352 Jouy-en-Josas cedex
Pierre.Catala@jouy.inra.fr
13 octobre 2003

Résumé

Un site d'enseignement supérieur et de recherche héberge souvent des unités de différents établissements entre lesquelles la mise en commun des moyens informatiques se limite à l'infrastructure du réseau local et à la connexion à l'Internet.
Il est donc difficile de regrouper en un lieu unique les serveurs des différentes unités qui ouvrent au moins une application à l'Internet. Dans ces conditions, le recours aux VLAN peut permettre de décentraliser la DMZ par sa répartition sur différents segments du réseau local.
Par ailleurs, certains établissements imposent à leurs unités distantes de se connecter via des VPN à certaines applications centrales. Ce n'est pas pour autant qu'il ne faut pas filtrer le contenu de ces tunnels chiffrés.
L'article présente une réflexion qui conduit à des évolutions envisageables de l'architecture réseau dont le but est de répondre à ces deux enjeux, plus qu'à une implémentation technique propre à un site.

Mots clefs

DMZ, cloisonnement, VLAN, 802.1Q, firewall, VPN, IPSec, SSH, SSL

1 Préambule

Un établissement d'enseignement supérieur et de recherche ou un organisme de recherche héberge différents types d'unités de recherche. Pour certaines, l'entité en charge de l'informatique collective et de la gestion réseau peut ne pas maîtriser totalement la politique d'accès depuis l'Internet. Ce constat concerne principalement les UMR (Unité Mixte de Recherche sous la tutelle de plusieurs établissements) et les unités qui ne dépendent pas de l'établissement qui les héberge. Ces interactions fortes avec d'autres établissements engendrent des contraintes au niveau de la sécurité du réseau local de l'établissement hôte.
Pour répondre aux attentes des unités sur les ouvertures d'applications à l'Internet et les communications avec d'autres établissements via des tunnels chiffrés, sans compromettre la sécurité informatique du site, différentes évolutions de l'architecture réseau sont envisageables.

2 Contraintes sur le réseau local d'un site multi-établissement

Les contraintes sur le réseau local d'un site multi-établissement, présentées ci-après, sont communes à de nombreux sites de l'INRA (Institut National de la Recherche Agronomique). Il est probable que cette description puisse s'appliquer à des sites d'autres établissements d'enseignement supérieur et de recherche.

L'INRA dispose de nombreux sites sur lesquels des unités d'autres établissements sont hébergées. Ceci complexifie la tâche des équipes du Service Infrastructure et Réseaux de l'INRA en charge de l'administration et de la sécurité des moyens informatiques collectifs.
Notamment, l'INRA a en commun des sites avec des écoles d'agronomie. Sur de tels sites où différentes populations d'utilisateurs se côtoient, il s'agit d'une co-gestion du réseau local et de la connexion Internet entre deux directions d'établissement et deux équipes informatiques.
D'autres sites INRA hébergent des UMR où les personnels INRA sont en minorité et dont la politique informatique est pilotée par un autre établissement de tutelle. Dans ce cas, il n'y a pas de co-gestion du réseau local. Il convient alors de concilier les besoins d'interconnexion entre l'UMR et ses autres établissements de tutelle avec le débit de la connexion à Internet et la politique de filtrage du site.

2.1 Serveurs ouverts à l'Internet éparpillés sur le site

Quelles que soient les composantes particulières du site, écoles ou UMR, il héberge des unités qui disposent de leurs propres serveurs. Ceux-ci offrent des applications à l'Internet, tels des serveurs Web, des serveurs FTP, des serveurs bases de données, des serveurs SSH ou d'autres applications de contrôle à distance de machines d'acquisition… Selon le site, le

nombre de serveurs ouverts à l'Internet est variable. Quel qu'il soit, dans la plupart des cas, il est inenvisageable d'héberger tous ces serveurs dans une même salle machine, pour créer une DMZ limitée à un seul segment réseau indépendant du réseau local. Pour certains, il est impossible de les déplacer puisqu'ils doivent être sur le lieu d'acquisition des données. Globalement, il n'est pas souhaitable de les déplacer car il est nécessaire de limiter l'accès physique de chaque serveur à ses administrateurs et la proximité est appréciable pour les interventions matérielles. Une salle machine qui regrouperait tous les serveurs ouverts à l'Internet du site ne permettrait pas cela. Elle obligerait la mise en œuvre d'une délégation de service auprès des personnels qui la géreraient.
A partir de ces constatations, l'organisation à mettre en œuvre pour un hébergement mutualisé des serveurs ouverts à l'Internet est coûteuse en moyens et en temps. Une évolution de l'architecture réseau est envisageable dans certains cas et peut être plus aisée à mettre en œuvre.

2.2 Déploiement non-maîtrisé de VPN depuis les postes de travail

Les unités sous la tutelle d'autres établissements doivent accéder à des applications hébergées par ceux-ci. Cela concerne notamment les applications administratives et s'étend de plus en plus à des applications scientifiques. Dans le cadre de projets scientifiques, cela concerne même des unités exclusivement INRA pour l'accès à des applications hébergées chez des partenaires.
Les contraintes imposées par les établissements tiers deviennent importantes pour sécuriser les communications entre les postes de travail hébergés sur des sites INRA et leurs propres serveurs. Actuellement, la tendance est à un fort déploiement de VPN IPSec avec l'installation de leurs clients sur des postes de travail INRA. Pourtant, les VPN cachent de nouvelles possibilités d'intrusion sous l'apparente facilité de déploiement et l'impression d'avoir sécurisé l'accès aux applications ouvertes à l'Extranet (périmètre défini de postes de travail externes). En effet, le mécanisme d'authentification supplémentaire qui peut être lié au serveur VPN et le chiffrement de la communication ne filtrent pas les sessions qui passent au travers du VPN. Un VPN peut donc court-circuiter le filtrage mis en œuvre sur les firewalls qui relient les deux sites entre lesquels il est établi. Ainsi, chaque extrémité de VPN sur un poste de travail peut être un point d'entrée non filtré sur le réseau local.
Par conséquent, différentes évolutions de l'architecture réseau sont envisageables : soit par l'isolement du reste du réseau local des postes de travail qui hébergent un client VPN IPSec ; soit par l'aménagement de l'accès aux VPN IPSec ; soit par la mise en œuvre d'une solution mieux adaptée aux besoins.

3 Où sont les risques ?

Il est ici question de risques réels dus à des failles connues et non de risques potentiels liés à ce que la fiabilité d'un logiciel ne peut être avérée et que le niveau de sécurité d'une machine baisse dès qu'elle est connectée au réseau.

La première mise en œuvre d'une politique de filtrage sur les sites INRA avait consisté à la fin des années 90 à identifier les applications ouvertes à des postes de travail externes au site qui les héberge. Celles-ci avaient été classées en deux catégories, celles ouvertes à l'ensemble de l'Internet et celles limitées à un Extranet.
Ce premier filtrage réalisé au moyen des listes de contrôle d'accès des routeurs n'avait pas permis de séparer du réseau local ces serveurs ouverts à l'extérieur. Il se limitait à une séparation entre l'Internet et le réseau local.
La méthode de filtrage employée, sur les routeurs et les firewalls utilisés, porte principalement sur les en-têtes IP et TCP/UDP. Elle consiste à contrôler les ouvertures de sessions pour limiter notamment l'accès direct depuis l'extérieur du réseau local à une liste définie d'applications. Par conséquent, les risques réels d'intrusion directe sont grandement atténués lorsque ces applications, ouvertes à l'Internet, sont mises à jour à l'occasion de la découverte de failles de sécurité. D'autant plus qu'il s'agit en grande partie d'applications "standard de l'Internet" (e.g., Apache) pour lesquelles leurs auteurs assurent un suivi rigoureux, à défaut qu'elles soient infaillibles.
Depuis la mise en œuvre de la première politique de filtrage, le nombre d'intrusions via une faille d'une application "standard de l'Internet" volontairement ouverte a fortement diminué. Néanmoins, il y a toujours énormément de tentatives d'exploitation de failles connues et toute ouverture accidentelle du filtrage, même de quelques minutes, est payée en retour par une intrusion. En effet, cela prouve, s'il était nécessaire de le démontrer, que les correctifs de sécurité sont rarement appliqués aux applications, même "standard de l'Internet", hébergées sur les machines dont l'usage est restreint au réseau local. Celles-ci sont donc faillibles à des attaques par rebonds véhiculées par une machine ouverte à l'Internet.

A l'analyse du mode opératoire des compromissions subies et sans tenir compte du nombre d'intrusions, il est évident que le risque réel s'est déplacé vers les applications Web et les postes de travail. Ces deux catégories ont en commun la difficulté d'administration. Il est bien plus difficile de les mettre à jour lors de la découverte de failles de sécurité comparativement aux quelques applications "standard de l'Internet" ouvertes à l'extérieur.

3.1 Risques liés aux applications Web

Pour les applications Web, le risque provient du fait qu'il s'agit pour une bonne part d'applications "maison" développées à un instant donné pour répondre à un besoin spécifique. Celles-ci font rarement l'objet d'une programmation rigoureuse et d'un suivi. Pourtant, cela permettrait d'éviter des failles de sécurité ou tout du moins de les corriger.
En outre, les applications Web peuvent recourir à des composants externes, être construites au moyen d'une boîte à outils ou développées dans une solution intégrée de micro-informatique qui réunit langage/base de données/serveur Web… Par conséquent, il est difficile de les appréhender en termes de sécurité avec cette variété d'éléments qui les compose.
Au minimum, un administrateur de serveur Web se doit de connaître la liste des éléments qui compose les applications hébergées pour réagir lorsque l'un d'eux est concerné par une faille (e.g., faille de type "Cross Site Scripting" dans la fonction start_form() du module Perl CGI.pm en septembre 2003). Néanmoins, cela est insuffisant sans suivi des applications. En effet, la mise à jour d'un élément faillible peut être impossible, si elle nécessite un changement de version qui impose une modification de l'application qui l'intègre.
Il est donc fort probable qu'un serveur Web héberge une application faillible. Par exemple, elle peut l'être à l'un de ces deux types de faille couramment rencontrés.

- L'accès à des fichiers hors de l'arborescence du service Web (directory traversal) peut permettre de récupérer des fichiers sensibles d'administration du serveur (e.g., iPlanet Directory Server 5.1 en juin 2003). Ceci peut se produire si l'environnement d'exécution de l'application Web n'est pas limité et si celle-ci a une faille dans l'analyse de la partie de l'URL qui lui incombe. Les fichiers ainsi récupérés peuvent révéler des informations utilisées ultérieurement pour réaliser une intrusion. A terme, l'attaquant vise à exécuter ce qu'il souhaite sur le serveur.
- L'exécution sur le serveur Web de codes arbitraires est quant à elle plus directe en termes d'intrusion (e.g., usage de la directive "include" de PHP avec une variable en argument). Ces codes sont envoyés par l'attaquant au travers d'un formulaire, dont la saisie n'est pas filtrée et peut être interprétée par l'application Web. Après avoir commandé la récupération d'un outil, l'attaquant peut déclencher son exécution.

3.2 Risques liés aux postes de travail

Pour les postes de travail, le risque provient principalement de ce que les utilisateurs exécutent lors d'une consultation Web, d'un téléchargement ou d'une réception de message. Toutefois ce risque n'est pas uniquement lié aux utilisateurs. Même s'ils sont responsables de certains "doubles clics" malheureux, les failles de certains logiciels contribuent à fragiliser les postes (e.g., failles récurrentes dans Internet Explorer).
Par conséquent, il est difficile d'empêcher des attaques qui transitent par les postes de travail : soit elles se servent d'actes volontaires des utilisateurs (e.g., Sobig.F en août 2003) ; soit elles utilisent des failles des logiciels. En effet, les logiciels présents sur les postes ne sont que rarement mis à jour avec les correctifs de sécurité alors que leur mobilité augmente. Ceci les amène à changer de périmètre de sécurité entre les différents lieux de travail et de domicile (e.g., ver Blaster en août 2003).

3.3 Combinaison de risques réels

La combinaison des risques réels liés aux applications Web et aux postes de travail permet de se convaincre de la difficulté à les endiguer. Par exemple, une attaque de type "Cross Site Scripting (XSS)" utilise une faille dans une application Web pour abuser l'utilisateur.

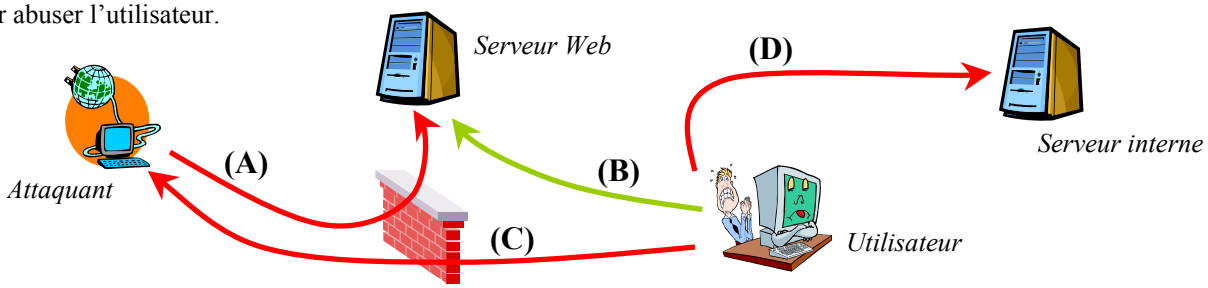

Figure 1 – *Attaque combinée*

L'attaquant (Figure 1), externe au site, saisit du code javascript dans un champ de formulaire (A). Ce code peut alors s'exécuter, quel que soit le système, sur un poste de travail interne au site. Ceci peut se produire si la saisie n'est pas filtrée par l'application Web et si un de ses utilisateurs consulte les entrées des visiteurs au travers de pages HTML (B). Ce code peut alors déclencher le téléchargement d'un cheval de Troie sur le poste de l'utilisateur (C) pour attaquer un serveur interne (D). Ce code peut aussi essayer de duper l'utilisateur (social engineering). A cette fin, un formulaire falsifié peut conduire l'utilisateur à révéler des informations confidentielles, tel un mot de passe.

4 Comment limiter la portée de ces risques réels ?

Au moins à court terme, il semble illusoire d'espérer fiabiliser toute application Web et changer les habitudes des utilisateurs. En outre, les risques réels, évoqués à la section 3, ne sont pas ponctuels comme celui lié à une faille sur une application "standard de l'Internet". En effet, pour cette dernière, le risque est ponctuel car généralement la livraison du correctif est rapide et son application est aisée. Ceci permet même d'envisager son arrêt pour une courte durée afin de limiter ce risque.
Comme ces mesures ne sont pas applicables aux applications Web et aux postes de travail, il convient de limiter la portée de ces risques réels à défaut de pouvoir les annihiler.

Un firewall de type passerelle d'application peut fournir un filtrage plus fin des communications, par une analyse des ordres liés à l'application, comparé à un firewall qui se limite au contrôle des ouvertures de sessions. Notamment, il peut permettre de filtrer certaines constructions de requêtes d'URL dont l'action néfaste est connue. Toutefois, son filtrage ne saurait parer à tout type d'attaque.
Force est donc de constater que le filtrage entre l'extérieur et l'intérieur d'un site ne sait limiter les risques réels sur les applications ouvertes à l'Internet. La seule manière de les endiguer est de corriger les failles connues. Malheureusement, cela n'est pas toujours aisément réalisable. Dès lors, il convient de limiter au maximum leur portée à l'intérieur du site. Ceci était moins crucial avec les applications "standard de l'Internet", si elles étaient rapidement corrigées.
Par conséquent, s'il n'est pas souhaitable de laisser ces serveurs au milieu du réseau local, la création d'une DMZ est rendue délicate par les contraintes liées aux caractéristiques des sites évoquées à la section 2. Effectivement, une seule DMZ est difficilement réalisable avec ces serveurs ouverts à l'Internet éparpillés sur le site. En outre, avec la prise en compte des risques liés aux postes de travail, il devient nécessaire d'étendre cette notion d'isolement des machines à risque. Plus exactement, il convient de définir des zones par classe de risque et de cloisonner le réseau local en fonction de celles-ci.

Le cloisonnement du réseau local est d'une difficulté nettement supérieure à la création d'une DMZ mais intrinsèquement il permet de la décentraliser.

5 Architectures de cloisonnement du réseau local

L'idéal ou l'ultime étape du cloisonnement du réseau local consiste à isoler chaque machine. Cette solution, qui est inenvisageable en l'état actuel, supprime même le besoin d'un firewall à la périphérie du réseau local. Ceci permet donc de l'ouvrir à l'interconnexion à haut débit. Un objectif moindre, plus réalisable actuellement, consiste à répartir le cloisonnement du réseau local sur les différents matériels qui constituent son infrastructure (i.e., firewall, routeur, switch).

5.1 Fonction firewall distribuée à toutes les machines

La notion de distribution de la fonction firewall à toutes les machines (Figure 2) permet : une maîtrise globale de la sécurité ; une grande précision de filtrage indépendamment de la topologie du réseau local ; une protection entre elles des machines du réseau local. En outre, cette architecture réalise le renforcement de la sécurité sans l'altération des flux à haut débit entre les machines internes et externes puisqu'il n'y a pas de passage par un matériel central de filtrage. [1]

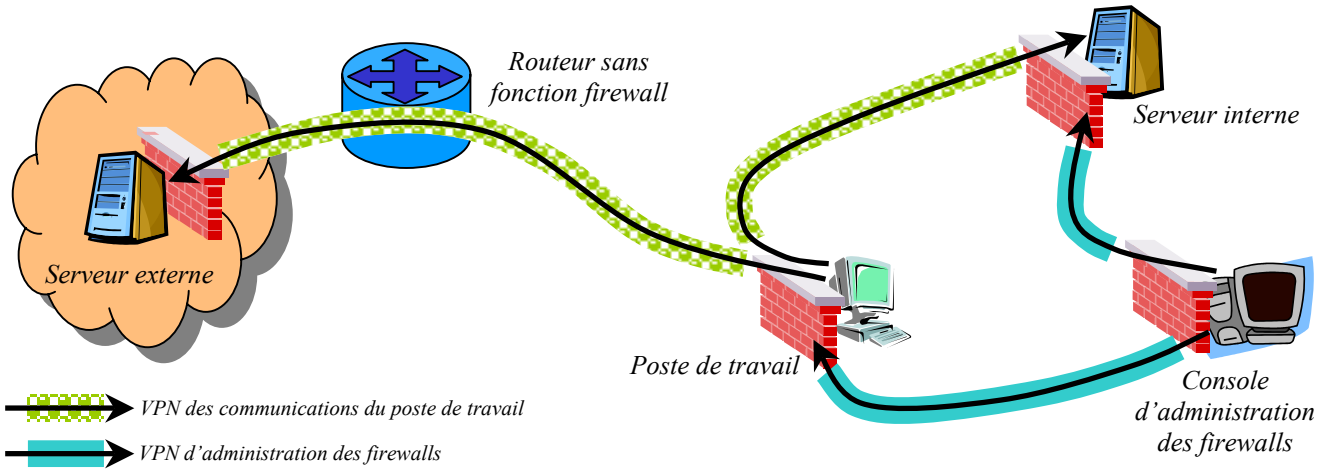

Figure 2 – *Fonction firewall distribuée*

La mise en œuvre de la distribution de la fonction firewall ne peut se faire qu'au moyen d'une administration centralisée, dont le but est de renforcer la sécurité. Elle rend la politique de filtrage lisible, cohérente et aisément modifiable pour en garantir la fiabilité.
Un outil d'administration centralisée, pour distribuer la fonction firewall à toutes les machines, n'existe pas actuellement. Dans les grandes lignes, cet outil pourrait assurer le stockage de la définition du filtrage de chaque machine au sein d'un annuaire. Ceci semble envisageable puisque certains éditeurs référencent déjà des machines au sein d'un annuaire pour publier les services qu'elles hébergent. Pour que le filtrage puisse être fiable et évolutif, le mode de stockage centralisé et structuré ne peut suffire. Encore faudrait-il que la définition du filtrage respecte le modèle objet. A savoir, la définition de quelques types de filtrage (assimilables à des objets) qui pourraient être appliqués à un grand nombre de machines (chacune aurait une instance de l'objet et recevrait toute modification du filtrage type). En outre, comme certaines machines, tels les serveurs, nécessitent un filtrage adapté pour répondre à des besoins spécifiques, il conviendrait de pouvoir particulariser certains types de filtrage (c'est la notion d'héritage).
Outre l'outil d'administration centralisée, il faudrait disposer sur toutes les machines d'un firewall intégré au système et suffisamment évolué pour supporter de nombreux protocoles d'application multi-session, voire analyser leurs ordres. Les communications entre les machines se feraient quant à elles au moyen de VPN IPSec avec authentification par certificats X.509. Ainsi les VPN IPSec participeraient à la fonction firewall et ne risqueraient plus de la court-circuiter puisque chaque extrémité de VPN IPSec serait intégrée à un firewall.

Bien qu'actuellement, cette architecture de cloisonnement reste théorique, ses objectifs et certains de ses concepts sont à prendre en considération.

5.2 Fonction firewall sur les matériels de l'infrastructure réseau

A défaut de pouvoir distribuer la fonction firewall à toutes les machines, sa distribution aux matériels de l'infrastructure réseau est plus envisageable actuellement. [2]

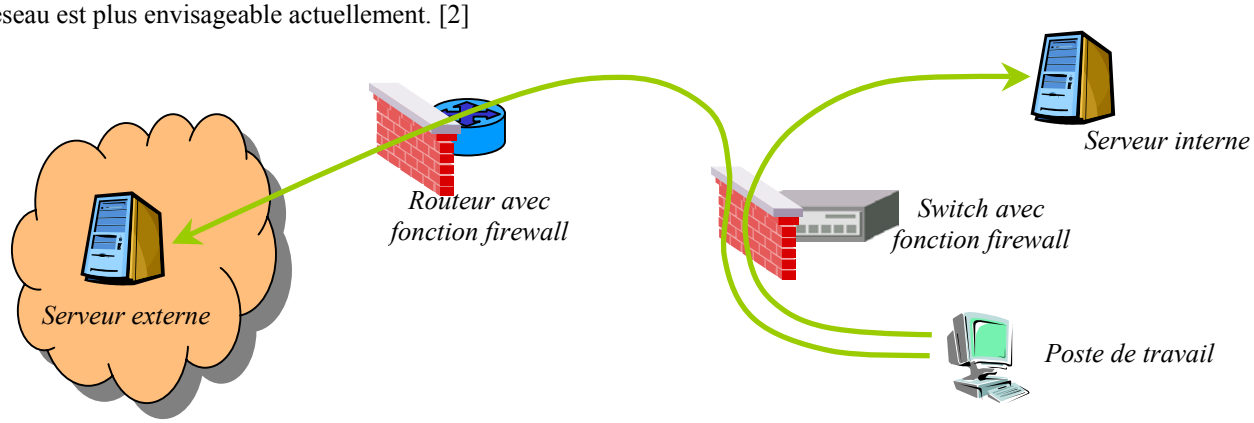

Figure 3 – *Fonction firewall sur les matériels de l'infrastructure réseau*

La mise en œuvre de la fonction firewall sur les matériels de l'infrastructure réseau (Figure 3) vise à maîtriser la sécurité globalement. Ceci est réalisé à partir de quelques points névralgiques pour éviter le déploiement complexe de solutions de contrôle au niveau des systèmes et des applications. Cette mise en œuvre consiste à répartir le filtrage au plus près des machines concernées pour limiter au maximum les flux parasites. Pour cela, elle recourt aux fonctions de filtrage embarquées dans les switchs, les routeurs et évidemment les firewalls.
Cette architecture de cloisonnement permet une précision importante du filtrage et nécessite une administration centralisée, tout comme l'architecture de distribution de la fonction firewall à toutes les machines.
En revanche, elle est très liée à la topologie du réseau. Ceci peut limiter la finesse de la protection entre les machines du réseau local au niveau de groupes de machines plutôt qu'au niveau de chaque machine comme pour la fonction firewall distribuée. Le filtrage mis en œuvre au niveau des matériels de l'infrastructure réseau peut aussi dégrader les flux à haut débit. En outre, cette architecture de cloisonnement est plus orientée sur l'autorisation des flux sur leurs points de passage que sur les autorisations d'émission et de réception des communications au niveau de chaque machine. Ceci peut rendre plus délicat la réplication d'un même type de filtrage à des machines connectées sur différents segments du réseau.
Des outils d'administration centralisée du filtrage réparti sur différents matériels de l'infrastructure réseau existent. Toutefois, chaque outil a une liste de matériels supportés relativement limitée. Ceci impose une première contrainte sur les matériels qui peuvent contribuer au filtrage réparti. Une deuxième contrainte porte sur les pré-requis en termes de filtrage. En effet, si la majorité des routeurs dispose de fonctions de base de filtrage, il n'en est pas de même pour les switchs. Cela

impose de disposer de switchs de niveau 3 aux fonctions étendues. En contrepartie, cette architecture de cloisonnement n'impose pas de pré-requis au niveau des machines.

Actuellement, ce type de cloisonnement est envisageable mais uniquement sur des infrastructures de réseaux locaux équipées de switchs de haut de gamme et de routeurs en leur sein.

6 Evolutions envisageables pour cloisonner le réseau local et maîtriser les VPN

Pour formuler des évolutions envisageables de l'architecture réseau, pour cloisonner le réseau local et maîtriser les VPN, il convient d'identifier des objectifs en fonction des caractéristiques des sites. En outre, il est nécessaire d'étudier comment certains concepts peuvent être déclinés sur les matériels qui constituent l'infrastructure réseau actuelle. Ces évolutions envisageables de l'architecture réseau portent sur la mise en œuvre de VLAN 802.1Q et sur un aménagement du déploiement des VPN.

6.1 Objectifs et concepts pour le cloisonnement du réseau local et la maîtrise des VPN

Les objectifs identifiés et les concepts proposés semblent plausibles en fonction des contraintes liées aux caractéristiques des sites évoquées à la section 2. Ils sont issus des deux architectures de cloisonnement évoquées à la section 5.

L'objectif principal est d'obtenir une meilleure maîtrise globale de la sécurité et sous-tend des objectifs secondaires afin d'augmenter la fiabilité du filtrage pour en renforcer la sécurité. Ces objectifs secondaires sont :

- de structurer la politique de filtrage en fonction de l'organisation des sites par établissements et par unités car les applications à ouvrir sont en partie liées aux unités ;
- de cloisonner les réseaux locaux selon des zones non topologiques mais définies par classe de risque (notion de DMZ décentralisée) pour isoler des groupes de machines en fonction du risque qu'ils représentent ;
- de faire abstraction de l'infrastructure réseau dans la définition du filtrage, ce qui permet de l'adapter plus aisément à certaines évolutions ;
- d'obtenir une bonne lisibilité du filtrage tant au niveau global du réseau qu'au niveau fin des machines ;
- de simplifier la mise en œuvre de la politique de filtrage pour pouvoir à la fois généraliser certains filtres et les rendre plus précis ;
- de contribuer à une meilleure cohérence de la politique de filtrage appliquée aux différentes unités des sites ;
- de réaliser aisément des modifications de filtrage applicables à des parcs de machines ;
- d'avoir un filtrage intégré aux extrémités des VPN IPSec pour qu'ils contribuent au cloisonnement ;
- de contrôler les débits pour privilégier ou limiter l'usage de certaines applications.

Au niveau concept, l'administration centralisée du filtrage et des VPN IPSec est incontournable pour atteindre l'objectif d'une meilleure maîtrise globale de la sécurité. Toutefois, il convient de limiter l'ampleur de son déploiement pour en assurer la réussite. A cette fin, l'administration centralisée doit reposer sur quelques matériels centraux de l'infrastructure réseau et le déploiement doit être réalisé par étapes. Celles-ci permettent d'affiner le cloisonnement dans le temps et en fonction de l'évolution des matériels qui constituent l'infrastructure réseau.
En contrepartie, les concepts évoqués ci-dessus peuvent pénaliser les flux à haut débit entre les machines internes et externes par la mise en œuvre sur des matériels centraux de filtrage.

6.2 Infrastructure réseau actuelle des sites INRA

Pour la mise en œuvre des objectifs identifiés, certains concepts sont proposés et il convient d'étudier la manière par laquelle il est envisageable de les décliner sur l'infrastructure réseau actuelle de l'INRA.

La politique de filtrage actuelle ne porte que sur la séparation entre le réseau local et l'Internet. Ainsi toute solution, qui permet de cloisonner un tant soit peu le réseau local, ne pourra que renforcer la sécurité.
L'infrastructure du réseau local est constituée uniquement de switchs de niveau 2. Elle ne comporte donc pas de matériels capables de réaliser du filtrage. Ses switchs supportent en majorité les VLAN 802.1Q. Les marques des switchs sont différentes selon les sites mais en règle générale ils sont homogènes à une marque par site.
Pour l'instant, aucun besoin ne semble avoir été émis en matière de hauts débits d'interconnexion interne-externe pour des applications spécifiques.

Les évolutions qui pourraient être apportées à l'infrastructure réseau actuelle doivent pouvoir s'appliquer par étapes au rythme des investissements en nouveaux types de matériels.
Notamment, elles pourraient reposer sur le renouvellement de la solution de filtrage. La solution retenue à l'INRA a été choisie principalement pour ses possibilités en termes d'administration centralisée du filtrage et des VPN IPSec. Une méthodologie de déploiement de cette solution a été définie pour structurer la politique de filtrage selon l'organisation des sites par établissements et par unités. Cette méthodologie vise à faire abstraction de la topologie du réseau et à rendre la politique de filtrage lisible, homogène et aisément modifiable par différents administrateurs. Elle permet une homogénéité entre les sites pour réaliser un filtrage précis et faciliter les autorisations aussi bien de type inter-site ou de type intra-site.

La méthodologie mise en œuvre pour le déploiement de la nouvelle solution de filtrage satisfait en grande partie les objectifs pour le cloisonnement du réseau local et la maîtrise des VPN. Il est donc envisageable d'étendre cette solution du filtrage de l'interconnexion interne-externe à un cloisonnement selon des zones par classe de risque.

6.3 Cloisonnement du réseau local au moyen de VLAN

Pour cloisonner le réseau local, un firewall ne peut suffire. Dans le cas, où la sécurité attendue n'exige pas de bâtir le cloisonnement uniquement sur des matériels qui réalisent du filtrage, il est envisageable de recourir aux VLAN 802.1Q. Ceux-ci permettent d'appliquer le cloisonnement selon des zones par classe de risque dans les multiples ramifications du réseau local. Ainsi, ils permettent de prolonger et de démultiplier virtuellement les interfaces du firewall central.

La configuration des VLAN par ports peut se faire par étapes et bien qu'il s'agisse d'une opération fastidieuse, il est possible de la rendre relativement stable pour éviter des adaptations fréquentes. Pour cela, il est nécessaire d'avoir peu de zones. Certaines zones seront liées à des classes de risque, d'autres à des unités du site. En outre, la mise en œuvre de ces zones est réalisable par étapes, à commencer par la DMZ décentralisée. Dans un premier temps, la plupart des postes de travail restent dans le VLAN par défaut. Ceci peut ensuite être appliqué aux bornes WiFi, dont le déploiement est quasiment interdit actuellement. Un isolement des machines mobiles est souhaitable à terme et peut être envisagé selon ce modèle.

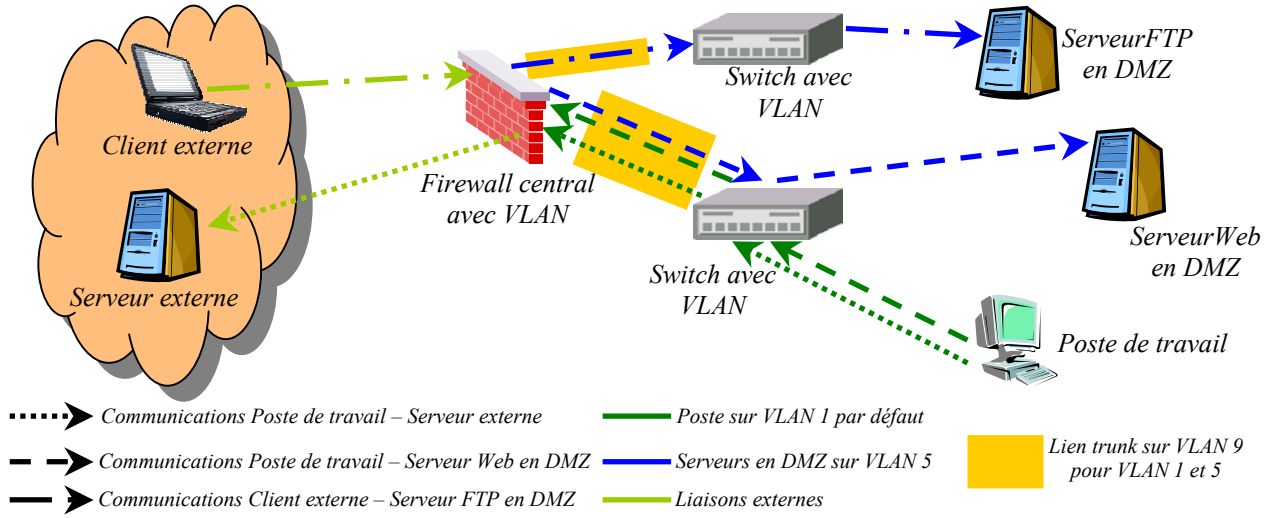

Figure 4 – *DMZ décentralisée*

A la création de la DMZ décentralisée qui héberge les serveurs ouverts à l'extérieur (Figure 4), il est nécessaire de positionner les applications selon qu'elles soient accessibles à l'extérieur ou limitées au réseau local. Ceci peut conduire à devoir déplacer des applications entre les serveurs ouverts et les serveurs internes. Cette même problématique de positionnement des applications se retrouve à toute création de zones.
Lors du placement des machines dans les différentes zones, il convient d'être attentif aux flux à hauts débits engendrés par les applications utilisées au sein du réseau local pour ne pas saturer le firewall central. Notamment, il convient de mettre un serveur de partages disques dans la même zone que ses postes de travail clients. Ceci nécessite de le protéger des postes par la configuration de son mécanisme de filtrage.

Pour permettre cette extension du firewall central au cloisonnement du réseau local, il convient que celui-ci supporte les VLAN 802.1Q. Ceci a pour principal intérêt de pouvoir transmettre l'information du numéro de VLAN au moyen d'un lien de type "trunk". Ainsi avec une seule interface, le firewall peut interconnecter plusieurs VLAN. Ceci est loin d'être négligeable au niveau de l'investissement en matériel.

Si le firewall peut fonctionner en mode "bridge", autrement appelé mode transparent, et assurer une communication filtrée entre VLAN sans nécessiter du routage, ceci permet d'éviter de revoir le plan d'adressage IP. Cette révision n'est pas une tâche mineure au niveau d'un réseau local.

Bien qu'en termes de sécurité, le cloisonnement du réseau local au moyen de la combinaison d'un firewall central et de VLAN 802 .1Q soit déconseillé, ceci est néanmoins une évolution envisageable de l'architecture réseau. Ce type de cloisonnement permet tout de même de renforcer la sécurité par rapport à un réseau non cloisonné. Par exemple, cela est suffisant pour limiter la propagation des vers actuellement connus. En effet, ceux-ci peuvent être introduits au sein du réseau local par des machines mobiles alors qu'ils sont bloqués par le firewall à la périphérie du site.
En outre, cette combinaison d'un firewall central et de VLAN peut être une première mise en œuvre du cloisonnement. Sans viser une meilleure sécurité, celle-ci permet déjà d'organiser le réseau local selon son usage pour limiter le trafic parasite (e.g., broadcast), ainsi que pour simplifier et rendre plus lisible le filtrage. Ce cloisonnement peut ensuite monter en niveau de sécurité par le déploiement de matériels de filtrage complémentaires au sein du réseau local.

6.4 Maîtrise du déploiement des VPN

L'installation sur les postes de travail du site, de clients VPN IPSec requis par des tiers, porte atteinte à la sécurité du réseau local. Il convient donc d'en maîtriser le déploiement et d'appliquer des solutions les plus en adéquation avec les besoins.

Un des modes de fonctionnement des clients VPN IPSec est nommé "split-tunneling". Ceci consiste à router au travers du tunnel VPN IPSec les communications du poste de travail à destination du tiers qui le requiert. En revanche, les autres communications continuent à transiter de manière classique au sein du réseau local. Ce mode de fonctionnement peut permettre de transformer le poste du client VPN IPSec en routeur et ainsi court-circuiter le filtrage à la périphérie du réseau local. En effet, des communications indésirables en provenance du tiers peuvent transiter par le tunnel VPN IPSec, sans pouvoir être filtrées par le firewall. Le poste client VPN IPSec peut alors les router à destination du réseau local. Ainsi, un serveur confidentiel interne au site peut être malencontreusement accessible à un tiers. A noter, des communications en sens inverse sont aussi possibles pour s'introduire anormalement dans le réseau local du tiers. Toutefois, le tiers a l'avantage de pouvoir maîtriser son VPN IPSec.
Par ailleurs, la maîtrise du client VPN IPSec pour activer du filtrage en sortie du tunnel semble difficilement envisageable. En effet, dans la majorité des cas, le client VPN IPSec est imposé par le tiers. Ceci est dû au fait que le système d'authentification des clients auprès du serveur VPN IPSec n'est pas standardisé et est donc propriétaire. Pour contourner le choix imposé du client VPN IPSec, il faut recourir à l'usage d'une clef partagée. Elle n'est pas pratique en termes d'usage et elle risque d'être refusée par le tiers, puisqu'elle diminue le niveau de sécurité du VPN IPSec.

Cette possibilité de créer un tunnel qui transporte un protocole à l'intérieur d'un autre s'étend à d'autres protocoles, notamment SSH et HTTP. Par exemple, elle est aisée à mettre en œuvre via une connexion interactive de type émulation de terminal qui donne accès à un shell. Avant la généralisation des accès PPP, cela était d'ailleurs fréquemment utilisé pour établir une session POP3 afin de relever les boîtes aux lettres via une connexion de type terminal.
En outre, pour un site qui ne filtre pas les connexions sortantes, rien ne limite l'installation d'un outil sur un poste de travail. Celui-ci établit directement la communication vers un serveur à l'extérieur sans recourir à un tunnel. Ce dernier peut alors lui envoyer des commandes pour atteindre des serveurs dont l'accès est strictement réservé au site.

A noter, il est possible de rendre récursif l'usage des tunnels. Dans ce cas, même un filtrage en extrémité de tunnel VPN ne peut rien contre un flux transporté au sein d'un tunnel réalisé au moyen d'un protocole qu'il autorise.

Les possibilités présentées ci-dessus relativisent le risque de communications indésirables au sein d'un VPN IPSec puisque ce n'est qu'un moyen parmi d'autres de véhiculer ce type d'attaque. Néanmoins, ce n'est pas pour autant qu'il faut renoncer à maîtriser les VPN car il est toujours souhaitable de maîtriser un risque.
En outre, sans se focaliser sur l'aspect sécurité, une non-maîtrise des VPN IPSec n'est pas souhaitable pour conserver la cohérence du réseau local. En effet, cela multiplie des points d'interconnexion virtuels mais qui sont réels au niveau IP. Ceci peut entraîner des perturbations sur le réseau local en cas d'une mauvaise configuration de l'un d'eux.

Pour les VPN IPSec établis par des utilisateurs de l'établissement à partir de l'extérieur vers le serveur VPN IPSec du site, la problématique est plus simple en termes de sécurité. En effet, dans ce cas, c'est l'établissement qui maîtrise le VPN IPSec et non un tiers. Ceci lui permet de définir la configuration du poste client VPN IPSec, notamment le filtrage qu'il embarque pour s'isoler du réseau qui lui fournit la connexion. En outre, le plus important est que cela permet à l'établissement de filtrer les connexions qui transitent par le tunnel. Cela est réalisé à l'extrémité du tunnel sur le serveur VPN IPSec puisqu'il est intégré au firewall.

Outre l'aspect sécurité, il convient de filtrer les communications qui transitent au travers des VPN afin d'éviter certaines aberrations pour des connexions de type WAN, tel l'accès à des partages de disques.

Pour éviter le recours systématique à des VPN IPSec qui assurent le prolongement du réseau local, des solutions alternatives visent à chiffrer un ensemble de sessions. Pour les distinguer, ces solutions sont qualifiées de sessions chiffrées et non de VPN.
Pour les connexions interactives de type émulation de terminal ou de type X11 et pour le transfert de fichiers, SSH peut être une solution. Il a l'avantage d'être actuellement mieux maîtrisé. Toutefois, il propose un mécanisme qui permet de transporter un autre protocole pour rediriger sa session. Ainsi, depuis le réseau d'un tiers, il est donc possible d'accéder aisément à des applications internes au réseau local, qui sont normalement interdites d'accès depuis l'extérieur.
Pour l'accès à un espace de documents, ce qui est fréquent dans les collaborations de recherche, la solution la mieux adaptée semble être un serveur HTTPS qui héberge cet espace. Dans ce cas, seul un navigateur Web est nécessaire sur le poste de l'utilisateur. Ainsi, la transmission des documents est réalisée en HTTP chiffré dans un tunnel SSL.
Pour l'accès aux boîtes aux lettres, la solution la mieux adaptée est le recours à POP3S ou IMAPS. Dans ce cas, il est nécessaire d'avoir, ce qui est maintenant courant, un client de messagerie qui supporte POP3S ou IMAPS sur le poste de l'utilisateur. La récupération des courriers est alors réalisée en POP3 ou IMAP chiffré dans un tunnel SSL.

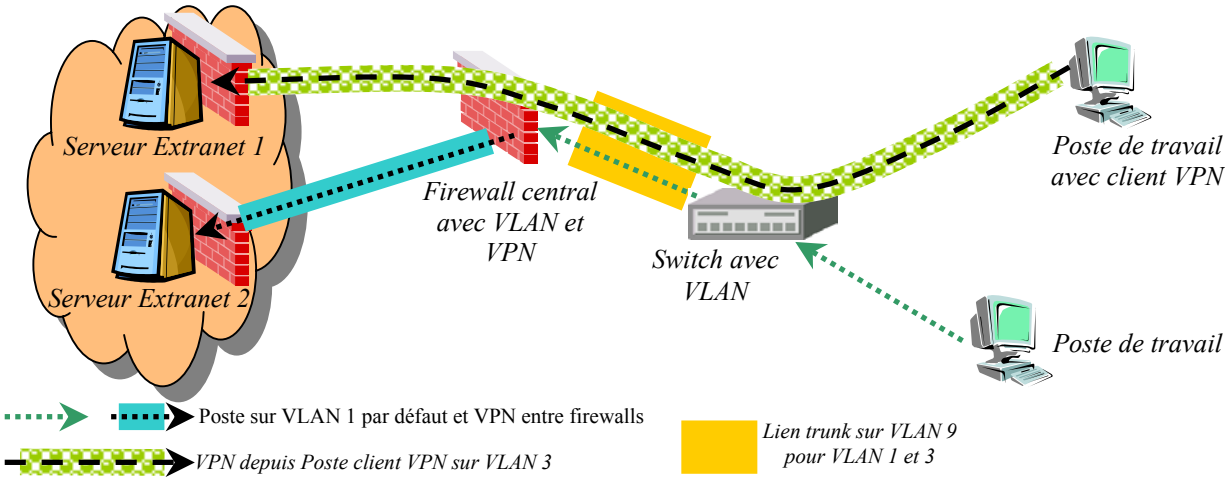

Figure 5 – *Architecture VPN*

Par conséquent, certaines évolutions de l'architecture réseau sont envisageables pour que les VPN IPSec s'intègrent et contribuent au cloisonnement du réseau local (Figure 5). D'ailleurs, une fois maîtrisé, un VPN IPSec est préférable à une solution SSH, pour laquelle il est difficile de maîtriser les redirections de sessions dans le cadre d'une gestion globale de la sécurité.

- Lorsque la mise en œuvre d'un client VPN d'un tiers est incontournable, il convient de déplacer le poste client VPN dans une zone classée à risque et non connectée directement au cœur du réseau local. Ceci nécessite l'existence du cloisonnement évoqué à la section 6.3.
- Lorsque le tiers souhaite des communications chiffrées entre les 2 sites, sans pour autant vouloir les maîtriser à partir du poste client, il est envisageable de déporter la gestion du VPN sur le firewall central. Celui-ci se charge alors d'établir le tunnel avec le serveur VPN du tiers. Toutefois, le tiers doit tolérer que les communications passent en clair à l'intérieur du réseau local. Autrement, il faut recourir à un premier VPN entre le poste client et le firewall central.
- Lorsqu'un VPN est requis par un tiers pour l'ensemble de ses communications avec une unité du site, il convient d'isoler le réseau de cette unité du reste du réseau local. Ceci nécessite l'existence du cloisonnement évoqué à la section 6.3 pour isoler le réseau de cette unité et déporter la gestion du VPN sur le firewall central. Il est aussi envisageable d'installer un firewall complémentaire qui isole le réseau de cette unité et qui gère le tunnel VPN.

7 Est-ce raisonnable d'utiliser les VLAN 802.1Q pour cloisonner ?

La question "Est-ce raisonnable d'utiliser les VLAN 802.1Q pour cloisonner ?" a déjà été posée quelquefois dans des listes de messagerie qui traitent de sécurité, notamment pour la création d'une DMZ. Certaines réponses sont nuancées, mais en règle générale, il y a un *a priori* négatif. [3] [4]

Les VLAN 802.1Q ont été conçus pour une optimisation du réseau local afin de limiter le trafic parasite et non à des fins de sécurité. Il semble qu'il n'y ait pas à attendre d'amélioration de la sécurité des switchs et des VLAN 802.1Q car le groupe IEEE 802.10 qui travaillait à leur sécurité a été mis en sommeil. Ses travaux n'ont pas été adoptés par l'industrie.
En outre, le niveau de sécurité sur l'ensemble d'une infrastructure est équivalent à celui de son équipement le plus faible. Cela signifie que faire reposer le cloisonnement du réseau local à la fois sur un firewall central et des VLAN 802.1Q conduit le niveau de sécurité global à être équivalent à celui des switchs et des VLAN 802.1Q. Par conséquent, peu importe la qualité du firewall, puisqu'il peut être "court-circuité" par des failles sur les switchs ou sur les VLAN 802.1Q.

Il convient donc d'évaluer les failles possibles sur les switchs et sur le mécanisme des VLAN 802.1Q utilisé pour cloisonner. Cette évaluation permet de définir les limites et les conditions d'usage des VLAN 802.1Q pour cloisonner le réseau local dans le but d'en renforcer sa sécurité.

7.1 Quelles sont les failles sur les switchs ?

Les switchs peuvent être faillibles à deux familles d'attaques. Les unes visent l'intégrité de la configuration du switch. Les autres visent à dérouter certains flux réseaux.

Pour leur administration à distance, les switchs nécessitent de disposer d'une adresse IP. Cela les rend donc sensibles à des attaques par le réseau. [5]
Ces attaques des switchs par le réseau visent : soit à modifier leur configuration via des protocoles non sécurisés (e.g., telnet, HTTP, SNMP) utilisés pour leur administration ou via une faille de leur système qui ouvre une porte dérobée ; soit à perturber leur fonctionnement par des attaques de type DOS auxquelles leur système est sensible.

Le but de dérouter certains flux réseaux sur les switchs est de pouvoir écouter certaines communications qui ne transitent pas normalement sur le port du switch auquel est connectée la machine de l'attaquant. Pour dérouter un flux réseau sur un switch, il existe deux techniques.

L'une consiste à effectuer une surcharge de la table du switch qui contient la liste des adresses MAC des machines connectées par port. Quand une telle surcharge se produit, la plupart des switchs se mettent à fonctionner comme des hubs ; ainsi tous les flux sont envoyés sur tous les ports. La réalisation d'une telle surcharge peut se faire au moyen d'outils qui génèrent une multitude de trames avec des adresses MAC différentes.
L'autre technique détourne la communication entre deux machines. Pour cela, la machine de l'attaquant envoie des fausses déclarations ARP pour usurper les adresses IP des deux machines dont il veut écouter la communication (spoofed ARP). Si ces deux machines acceptent les fausses déclarations ARP, elles enverront la communication vers la machine de l'attaquant. Cette dernière écoute ainsi la communication et la relaie pour qu'elle atteigne sa destination normale.

7.2 Quelles sont les failles sur les VLAN 802.1Q ?

Les failles sur les VLAN 802.1Q ne semble pas dues à des erreurs d'implémentation mais sont inhérentes à leur conception. En effet, les performances de commutation des switchs ont été privilégiées et certaines vérifications ne sont pas réalisées. Ceci peut permettre à une trame de forcer son passage d'un VLAN à un autre de manière anormale. [6] [7]

Le passage forcé par la trame entre deux VLAN, autrement appelé "saut de VLAN", pourrait être bloqué. Pour cela, il faudrait que la réception de trames marquées avec un numéro de VLAN (tagged frame) ne soit permise que sur les ports qui relient uniquement des switchs entre eux. En effet, les machines n'ont pas à émettre de trames marquées, c'est du ressort des switchs. Ces liens qui transportent des trames marquées pour assurer la continuité des VLAN sur plusieurs switchs sont dits de type "trunk". Comme le standard ne permet pas d'empêcher des liens de type "trunk" sur les ports auxquels sont connectées les machines, toute machine peut donc injecter des trames marquées.
En outre, il faudrait que les switchs analysent les trames marquées qui transitent entre deux de leurs ports même s'ils appartiennent au même VLAN. L'absence de cette vérification est due à des raisons d'optimisation de la vitesse de commutation et permet de véhiculer entre switchs des trames marquées qui ont été injectées par des machines.

Ces vérifications absentes du standard 802.1Q n'ont malheureusement pas été ajoutées dans son amendement 802.1u. [8]

Ces absences de vérification permettent donc à une machine attaquante d'injecter une trame marquée à destination d'une machine cible qui appartient à un autre VLAN. Cette trame est marquée anormalement avec le numéro du VLAN de la machine cible. Lorsqu'elle arrive sur le switch auquel est connectée la machine attaquante, elle est envoyée sans vérification

vers le switch auquel est connectée la machine cible. Ceci se produit, si le VLAN de la machine attaquante est le même que le VLAN de base du lien de type "trunk" entre les switchs. En outre, cette attaque n'est possible qu'entre deux machines non connectées au même switch.

Le passage forcé par la trame entre deux VLAN ne permet que d'envoyer dans un sens des trames entre deux machines qui appartiennent à des VLAN différents. Pour que le retour soit possible, il faut qu'il y ait une erreur de configuration dans l'équipement qui assure le filtrage entre les VLAN.
Il convient donc de relativiser ce risque qui peut être endigué par une configuration correcte des VLAN. En effet, il suffit que le numéro du VLAN de base des liens entre switchs ne soit pas attribué à des ports auxquels sont connectées des machines.

7.3 Limites et conditions d'usage des VLAN 802.1Q

Les risques semblent être plus liés aux switchs qu'aux VLAN 802.1Q. Il convient donc d'étudier quelles sont les mesures envisageables pour utiliser les switchs et les VLAN à des fins de sécurité.

L'attention doit porter principalement sur les switchs.
Des mesures doivent être prises pour la sécurité du protocole qui permet l'administration des switchs à distance. Il est impératif d'utiliser un protocole dont les communications sont chiffrées et dont l'authentification ne se fait pas au moyen d'un mot de passe qui circule en clair sur le réseau. Si possible, il est souhaitable d'isoler les adresses IP d'administration des switchs sur un VLAN spécifique. En outre, il est impératif que les protocoles d'administration faillibles soient désactivés.
En ce qui concerne l'administration des switchs, il est impératif de les tenir à jour des évolutions de leur firmware et de changer leur mot de passe par défaut.

Au niveau de la configuration des VLAN 802.1Q, il est impératif d'utiliser un numéro spécifique pour le VLAN de base des liens de type "trunk" entre les switchs. Pour la configuration des ports auxquels sont connectées les machines, il est impératif de n'attribuer qu'un seul numéro de VLAN.
Exceptionnellement, un serveur peut être connecté à plusieurs VLAN pour limiter les flux qui transitent par le firewall central. Dans ce cas, il est impératif que les niveaux de sécurité des différents VLAN, auxquels il est connecté, soient à peu près similaires. En outre, le serveur ne doit pas permettre le passage de communications entre les VLAN pour ne pas "court-circuiter" le firewall central. Il convient aussi de renforcer la sécurité du serveur par un mécanisme de filtrage intégré à son système.

Pour ne pas diminuer le niveau de sécurité atteint par le filtrage entre l'Internet et le réseau local, il est impératif de ne pas partager un switch au moyen de VLAN entre le réseau externe et le réseau interne. En effet, en cas de dysfonctionnement du switch, ceci "court-circuite" le firewall à la périphérie du réseau local.

Malgré la prise en compte de ces principes de configuration des switchs et des VLAN 802.1Q, le risque le plus important demeure. En effet, il s'agit de la possibilité de détourner des communications.
Certains switchs disposent de mécanismes pour contrer l'attaque de surcharge de leur table qui contient la liste des adresses MAC des machines connectées par port. Notamment, ces déclarations peuvent n'être réalisées que par l'administrateur. Ces déclarations statiques sont toutefois fastidieuses à mettre en œuvre. Il est parfois possible de configurer le switch pour qu'il ne prenne que la première déclaration par port. Ceci n'est valable que pour les ports auxquels une seule machine est connectée. Certains switchs ne prennent pas en compte les nouvelles déclarations lorsque leur table est remplie. Par conséquent, ils bloquent toute trame émise par une machine qui n'a pu être prise en compte. Lorsque cela est possible, il convient de configurer les switchs pour que chaque VLAN 802.1Q dispose de sa propre table d'adresses MAC par port. Ceci permet d'éviter qu'une surcharge de cette table dans un VLAN n'impacte les autres VLAN.
En revanche, il est plus difficile de contrer l'attaque à base de fausses déclarations ARP. La seule solution consiste à disposer d'une table ARP statique sur chaque machine et à ne pas accepter les déclarations ARP dynamiques. Ceci semble inenvisageable. La seule solution raisonnable repose sur le firewall central à défaut d'avoir des switchs aux fonctions évoluées. Celui-ci peut signaler les nouvelles déclarations ARP qui rentrent en conflit avec les déclarations précédemment enregistrées dans sa table ARP. Cette solution permet d'alerter, voire de bloquer si l'usurpation vise une machine d'un autre VLAN 802.1Q. Malheureusement, au sein d'un même VLAN 802.1Q connecté à une seule interface du firewall, ce dernier ne peut pas bloquer l'attaque.

Pour sécuriser la mise en œuvre des switchs et des VLAN 802.1Q, certaines configurations sont impératives et nécessitent que certaines fonctions soient disponibles sur les switchs. Il convient donc d'évaluer chaque switch pour savoir s'il est envisageable de l'utiliser pour la mise en œuvre du cloisonnement du réseau local au moyen de VLAN 802.1Q.

8 Finalement, quelles évolutions de l'architecture réseau retenir ?

L'architecture de DMZ décentralisée et, de manière étendue, de cloisonnement par zone de risque, permet de répondre aux différents besoins d'interconnexion des unités de recherche. Ce principe d'architecture peut même s'appliquer avec des politiques de sécurité différentes entre les unités.

Il convient donc d'évaluer les niveaux de sécurité à mettre en œuvre en fonction des risques par zone de risque ou par unité. Toutefois, il convient de ne pas oublier, que le système informatique n'est qu'un élément parmi d'autres, auquel des mesures de sécurité doivent être appliquées. Cela signifie qu'il ne sert à rien de viser un cloisonnement du réseau local très fort en termes de sécurité si celle-ci n'est pas appréhendée globalement.
Pour une unité, cette prise en compte globale de la sécurité signifie qu'elle doit aussi porter sur la protection des installations et sur les procédures d'accréditation des personnes.
Pour l'infrastructure réseau, cela signifie une protection physique des baies de brassage et des matériels qui la composent.

C'est au niveau de l'implémentation de cette architecture que différentes options d'évolution existent. Celles-ci dépendent du niveau de sécurité visé. En effet, pour des unités qui ont appréhendé globalement la sécurité et qui requièrent une forte étanchéité avec le reste du réseau local, il convient de les séparer au moyen d'un firewall spécifique. Celui-ci doit être administré comme le firewall central. Pour le reste du réseau local, la mise en œuvre des VLAN 802.1Q et des VPN IPSec, selon les principes évoqués aux sections 6.3, 6.4 et 7.3, permet de renforcer la sécurité.

Références

[1] Steven M. Bellovin, Distributed Firewalls. *Login*, pages 37-39, Novembre 1999.
http://www.research.att.com/~smb/papers/distfw.html

[2] Hervé Schauer, Sécurité réseau distribuée – Du garde-barrière au cloisonnement de réseau.
Congrès JRES 1999, Montpellier, Novembre 1999.
Egalement publié dans Confidentiel Sécurité, 74 et 75, Janvier et Février 2001.
http://www.hsc.fr/ressources/articles/cloisonnement/index.html.fr

[3] VLAN as a DMZ. Liste de messagerie Security Basics de SecurityFocus, Mars 2002.
http://www.securityfocus.com/archive/105/260310

[4] DMZ via VLAN. Liste de messagerie Firewalls de GNAC, Avril 2001.
http://archives.neohapsis.com/archives/firewalls/2001-q2/0070.html

[5] Aaron D. Turner, Network Insecurity with Switches. Site www.giac.org, Août 2000.
http://www.giac.org/practical/gsec/Aaron_Turner_GSEC.pdf

[6] IEEE, Virtual Bridged Local Area Networks. IEEE Std 802.1Q-1998, Décembre 1998.
http://standards.ieee.org/getieee802/download/802.1Q-1998.pdf

[7] David Taylor, Are there Vulnerabilities in VLAN Implementations? Site www.sans.org, Juillet 2000.
http://www.sans.org/resources/idfaq/vlan.php

[8] IEEE, Virtual Bridged Local Area Networks – Amendment 1: Technical and editorial corrections.
IEEE Std 802.1u-2001, Mars 2001.
http://standards.ieee.org/getieee802/download/802.1u-2001.pdf