

## La sécurité réseau distribuée

### Références

■ Sur la sécurité par le filtrage IP : *Le Cloisonnement de réseau*, Hervé Schauer, HSC, Infosec juin 1997. <http://www.hsc.fr/ressources/presentations/part/>  
*Du Garde-Barrière au cloisonnement de réseaux*, Hervé Schauer, Journées Réseau du CNRS. <http://www.hsc.fr/ressources/presentations/jres99/jres99.html>  
 Cours sécurité réseau distribuée par Hervé Schauer : <http://www.hsc.fr/ressources/presentations/dns/>  
*Thinking beyond firewalls & IDS : the Network Sentry*, de John Flowers & Tom Stracener, Hiverworld, SANS Network Security, October 1999. [http://www.sans.org/Distributed Firewalls](http://www.sans.org/Distributed%20Firewalls), by Steve Bellovin, ATT Research <http://www.research.att.com/~smb/papers/>

■ Sur la détection d'intrusion : *Introduction à la détection d'intrusion*, par Stéphane Aubert <http://www.hsc.fr/ressources/presentations/ids-intro/>  
*Table ronde sur la détection d'intrusion à Infosec 2000*, par Hervé Schauer <http://www.hsc.fr/ressources/presentations/infosec2000/>  
*Tests d'ISS Realsecure et Cisco NetRanger*, par Hervé Debar (IBM Zurich) : <http://www.ossir.org/ftp/supports/99/debar/index.html>  
*État de l'art en détection d'intrusion*, par Ludovic Me (Supelec) : <http://www.supelec-rennes.fr/rennes/si/equipe/lme/perso/publi/x-aristote.pdf>

**Se reposer sur les caractéristiques propres des réseaux pour garantir leur sécurité, en intégrant les problématiques que soulèvent les intranets et les extranets, c'est la solution séduisante qu'offre le cloisonnement de réseaux, sans entraîner de frais importants ni de remise en cause de l'architecture existante.**

Les risques inhérents aux réseaux informatiques sont aussi nombreux que les utilisations potentielles. Il peut s'agir d'un stagiaire indélicat qui écoute le réseau à l'insu des utilisateurs, d'un concurrent qui tire parti d'une collaboration ponctuelle pour accéder à des données confidentielles. Mais sans parler de piratage, comment prévenir la grève d'employés mécontents, ayant pris connaissance sur le Web interne d'une filiale étrangère, des avantages accordés à leurs collègues du pays voisin ? Comment se protéger face à une telle diversité des risques ? Installer une multitude de *firewalls* pourrait apparaître comme la solution, mais cette option est finalement peu réaliste, ne serait-ce que sur le plan financier. De plus, la logique d'un *firewall* est souvent binaire : sur le réseau « intérieur » du *firewall*, toute donnée est considérée comme autorisée à sortir. Sur le réseau extérieur, toute donnée est considérée comme potentiellement hostile. Cette logique est de plus en plus souvent prise en défaut, ne serait-ce qu'avec le développement des extranets, qui autorisent des intrus potentiels à accéder à « l'autre côté » des *firewalls*.

Entre l'alternative qu'ont les responsables de sécurité de laisser le réseau ouvert aux quatre vents ou d'acheter et de déployer des *firewalls* coûteux et obtenir quoi qu'il en soit une sécurité incom-

plète, une troisième option est envisageable. Il s'agit simplement de tirer parti du réseau lui-même. Les réseaux sont en effet construits à partir d'éléments possédant des capacités de filtrage, typiquement les routeurs et les commutateurs, et permettant donc de mettre en place une sécurité distribuée au niveau du réseau.

La mise en place d'une telle sécurité passe par un cloisonnement du réseau <sup>(1)</sup>. Cette solution présente des avantages non négligeables : pas de bouleversement de l'architecture, pas d'ajouts systématiques de machines. Pour cloisonner un réseau il suffit de le découper en ensembles de sous-réseaux, les domaines, puis de mettre des filtres sur les routeurs ou les commutateurs qui interconnectent ces sous-réseaux. Les périphériques qui font du filtrage dans le réseau deviennent des SPEP (*Security Policy Enforcement Points*). Les périphériques filtrants ne laissent passer que les flux nécessaires entre les domaines, en utilisant des ACL (*Access Control Lists*) classiques.

Les applications du cloisonnement de réseau sont nombreuses car dès que plusieurs systèmes de filtrage sont nécessaires, le cloisonnement est intéressant. Cela peut être la sécurisation au sein d'un intranet entre les différents services et projets, la gestion d'accès complexes à Internet, les plateformes de commerce électronique, les extranets ou les réseaux en étoile. Le cloisonnement de réseau est la brique de base vers l'usage de tunnels chiffrés IPsec, qui reposent sur une sélection des flux, et vers le déploiement de la sécurité sur les individus, par le lien d'un individu à l'adresse IP de son PC. ■

(1) Le cloisonnement de réseau est aussi appelé le partitionnement de réseau (*network partitioning* en anglais).

### SÉCURITÉ APPLIQUÉE AU NIVEAU RÉSEAU PAR RAPPORT À LA SÉCURITÉ APPLIQUÉE AU NIVEAU SYSTÈME D'EXPLOITATION ET APPLICATIFS

Niveau OS & applicatif

- Configuration de la sécurité dans beaucoup d'applications,
  - Configuration de la sécurité dans beaucoup de serveurs de manières diverses,
  - Impacte beaucoup d'administrateurs de serveurs et d'applications dans de nombreux endroits,
  - Difficile à implémenter sans un outil,
  - Difficile à implémenter avec les outils existants,
  - Difficile d'être cohérent d'un système ou d'une application à l'autre,
  - Coût élevé,
  - Application statique de la sécurité : l'accès est acquis à l'ouverture des fichiers du socket ou au lancement du processus. Si la permission change, l'accès est toujours acquis,
  - Pourra utiliser des certificats X.509.
- Exemple : Windows 2000.

Niveau TCP/IP

- Configuration de la sécurité une seule fois dans tout le système d'information,
  - Impacte le service de conception et le service de gestion du réseau,
  - Difficile à implémenter sans un outil,
  - Facile à implémenter avec les outils existants,
  - Cohérent de part le concept de globalité,
  - Coût moyen,
  - Application dynamique de la sécurité : l'accès est validé en temps réel sur le flux. Si la permission est supprimée, les sessions en cours sont stoppées,
  - Pourra utiliser des certificats X.509.
- Exemple : IPsec, SSL.

## Intégrer la sécurité comme service du réseau

**Face aux solutions traditionnelles et plus anciennes, le cloisonnement de réseau propose un nouveau concept de définition de la sécurité. Celle-ci peut désormais être déployée globalement et simplement sur le réseau, en devenant un service du réseau.**

Si la sécurité distribuée dans le réseau s'impose, il faut en chercher la cause dans le manque de pertinence des alternatives. Les solutions de sécurité réseau disponibles jusqu'à présent présentent des difficultés. La sécurité distribuée, basée sur Kerberos au niveau des systèmes d'exploitation, est complexe à mettre en œuvre, à administrer et à déployer. La principale version commerciale était OSF/DCE sur Unix, qui n'a jamais décollé. Dans Windows 2000, Microsoft propose un dérivé de Kerberos. Le contrôle d'accès de Microsoft utilise le champ optionnel « data authorization field » pour une information propriétaire et obligatoire, indiquant les privilèges d'accès entre le client et le serveur. Ceci interdit toute interopérabilité avec les Kerberos existants. Difficile à dire si ce dérivé de Kerberos aura du succès, car dans le même temps, Windows 2000 intègre une autorité de certification et des certificats X.509. Dans tous les cas, la caractéristique principale est la complexité globale de cet ensemble.

La détection d'intrusion peut se révéler utile dans certains cas : pour détecter des erreurs de configuration, des signatures dans le contenu de certains protocoles, ou pour pallier la journalisation incomplète des *firewalls*. Cependant, la détection d'intrusion est facile à contourner, par exemple en utilisant la fragmentation, et ce dans tous les cas. La détection d'intrusion est une sécurité passive, le principe est de regarder le trafic, et de détecter ce qui n'aurait pas dû passer. De plus, elle ne permet plus de détecter la compromission d'un composant du réseau. L'efficacité de la détection d'intrusion est principalement soutenue par un marketing omniprésent.

L'usage courant des RPC (*Remote Procedure Calls*), du code mobile et le développement des technologies objet et des architectures n-tiers, bouleverse les modèles de sécurité existants. L'infrastructure d'une entreprise n'est plus caractérisée par les applicatifs et les données, mais par les flux dans son réseau. Au lieu de se focaliser sur une application de la sécurité à des niveaux élevés (système d'exploitation, applications et données), il est devenu beaucoup plus efficace et réaliste de déployer la sécurité au niveau du réseau dans les flux d'information.

Au final, l'ensemble des techniques de sécurité existantes demeure indispensable, mais la sécurité réseau répartie par le cloisonnement de réseau est le concept d'avenir. Il peut-être vu comme la distribution dans le réseau de nombreux *firewalls*,

avec une gestion et vision globale. Pour autant est-ce une bonne solution ? Si vous posez la question à un gestionnaire de réseaux, aux centres de supervision et autres architectes, ils sont parfois dubitatifs. Mais dans la majorité des cas, et particulièrement en France, la sécurité représente en effet une sorte d'épouvantail pour ces personnes. En revanche, les administrateurs système et applicatifs, comprennent l'intérêt de la sécurité déployée dans le réseau, transparente pour eux et leurs utilisateurs. Le responsable sécurité retrouve une vision globale et simple de sa politique de sécurité. Il faut donc évoluer et comprendre que la sécurité est désormais un service du réseau.

### Le security policy management

La gestion au niveau politique implique le déploiement de la sécurité d'abord dans le réseau. Cette démarche de sécurité dans le réseau s'inscrit dans le cadre de ce qui se nomme outre-Atlantique le *security policy management*. La sécurité est en effet la première application concrète de cette révolution, le moteur économique du *policy management* demeurant la qualité de service. Loin d'être une invention marketing, ce concept correspond à un nouveau niveau d'abstraction. Le *security policy management* permet l'application des besoins de l'organisation sur l'ensemble de l'infrastructure réseau du système d'information. Cette vision véritablement globale permet ainsi de définir une politique de sécurité cohérente et évolutive, proche du langage des décideurs, tant en termes de taille que d'architecture. Ces deux caractéristiques sont la garantie d'une sécurité pérenne. Parmi les nombreux autres avantages de cette vision globale « politique », on peut citer la facilité de gestion, une gestion simplifiée qui permet une granularité accrue de la politique de sécurité. Une politique de sécurité définie à ce niveau global permet en outre de mieux protéger le réseau contre les attaques internes et autorise un contrôle accru des machines nomades.

On peut tenter de définir le fonctionnement du *security policy management* ainsi : une gestion centralisée et globale d'une architecture répartie et décentralisée. À l'instar d'un logiciel de gestion de réseau, la gestion de politique de sécurité réseau implique le maintien d'une base de connaissances sur la topologie du réseau, les caractéristiques des équipements, les serveurs d'authentification et les autorités de certification. La gestion au niveau politique ne se base généralement pas sur une connaissance de la topologie physique du réseau, mais bien plutôt sur celle de la topologie logique, cette dernière fournissant généralement une image plus fidèle des besoins réels de l'organisation. ■

Dossier réalisé par Hervé Schauer

[www.hsc.fr](http://www.hsc.fr)

### Zoom

Sécurité appliquée au niveau du périphérique ou au niveau global

Fragmentée, périphérique

- Ne permet pas de scalabilité,
- difficile à gérer,
- complexité qui provoque des trous de sécurité,
- complexité, interdit la granularité,
- configuration de la sécurité incohérente entre les périphériques,
- la configuration de sécurité devient statique,
- impossible d'appliquer la politique,
- ne protège pas contre les attaques internes,
- difficile de contrôler les nomades.

Centralisée

- Permet la scalabilité avec une vision globale,
- facile à gérer,
- complexité masquée par la simplicité de la politique,
- simplicité, permet la granularité,
- configuration de la sécurité cohérente par le design global,
- politique demeure à jour,
- permet l'application de sa politique,
- protège des attaques internes,
- permet plus facilement le contrôle des nomades.