Le Garde-Barrière HSC

par
Hervé Schauer et Christophe Wolfhugel

Herve.Schauer@hsc-sec.fr, Christophe.Wolfhugel@hsc-sec.fr

Hervé Schauer Consultants

Télécopie: (1) 46 38 05 05
Téléphone: (1) 46 38 89 90

Résumé

Les besoins de connectivité et de sécurité des organisations et entreprises ne cessent d'augmenter. Il devient donc nécéssaire de contruire et gérer des connexions Internet qui respectent les politiques de sécurité.

Ce document décrit une architecture de sécurité répondant à ce besoin : il propose une passerelle Internet sécurisée. Celle-ci intègre une methodologie permettant l'exploitation du Garde-Barrière, constituée d'au moins un routeur et une machine, avec eventuellement un logiciel d'identification et d'authentification.

Plan

I. Introduction
   - IP
   - L'Internet
   - Besoin de connectivité
   - Les risques
   - La solution

II. L'architecture de sécurité
   - Contenu
   - La démarche entreprise

III. Le Garde-Barrière

IV. Les machines agréées

V. Gestion des services applicatifs

VI. Exigences de sécurité pour le Garde-Barrière

VII. Exigences de sécurité pour les machines agréées

VIII. Identification et authentification
   - Fonctionnement
   - Configuration

IX. Conclusion
   - Organisation

I. Introduction

I.1 IP

IP est le protocole de routage de la suite de protocoles INTERNET ou suite de protocoles TCP/IP. IP est devenu le plus connu des protocoles et c'est le seul protocole inter-réseaux (conçu pour interconnecter des réseaux) répandu. La suite de protocoles INTERNET offre une qualité de services proposés à l'utilisateur inégalée, que ce soit en souplesse, facilité d'emploi, puissance, performance, variété, transparence, etc ... C'est pourquoi IP ne cesse de se développer dans le monde, et a été choisi par les opérateurs de télécommunications. C'est *le* protocole essentiel du moment, c'est pourquoi IP est le protocole pris en compte dans l'architecture décrite ci-après. De plus, une sécurité efficace préfère une plus grande simplicité et l'utilisation d'un seul protocole de réseau, aussi seul IP est considéré.

I.2 L'Internet

L'Internet est le réseau planétaire regroupant l'ensemble des machines communicant à l'aide du protocole TCP/IP et partageant le même espace d'adressage IP. Ce réseau, d'origine académique, regroupe aujourd'hui des réseaux privés et publics, de recherche (NSFnet, NREN, NorduNet, Renater, Fnet etc) et commerciaux (Uunet (réseau Alternet), PSI, etc). Il se développe rapidement dans le monde et même en Europe où une volonté politique d'orientation vers les protocoles ISO est toujours perceptible.

I.3 Besoin de connectivité

Les grandes entreprises et organisations mettent en place de grands réseaux IP et migrent de protocoles propriétaires vers IP. Elle ont besoin d'interconnecter au sein de l'entreprise des réseaux IP géographiquement éloignés, et vers l'extérieur de se connecter vers des partenaires et à l'Internet.

I.4 Les risques

Avec cette nouvelle connectivité, les risques vis-à-vis de la sécurité augmentent. Ils peuvent apparaitre à la fois parce que l'entrée depuis l'extérieur est facilitée, et parce que la sortie vers l'extérieur offre de nouvelles perspectives. C'est pourquoi il est indispensable de prendre en compte la sécurité. L'objectif est de trouver le bon équilibre entre les besoins de sécurité et la commodité d'utilisation de la connectivité IP.
Il faudra gérer des entités nouvelles, des ressources humaines, développer des actions de sensibilitation et formation, intégrer de nouveaux services pour les utilisateurs, savoir réagir en cas de problème, etc.

I.5 La solution

Afin d'atteindre cet objectif nous définissons une architecture de sécurité qui permet d'organiser la sécurité d'une connectivité IP entre une entité à protéger et le reste du monde. Cette architecture propose :

- des exigences à suivre (techniques, humaines, etc),
- des cahiers de recettes permettant de valider les exigences,
- des solutions techniques, intégrant un système d'identification et d'authentification des utilisateurs.

Ces solutions techniques reposent sur la conception d'une passerelle IP sécurisée appellée **Garde-Barrière**. Elle est constituée au minimum :

— d'un routeur IP,

— d'un serveur UNIX.

Elle sert de passerelle sécurisée ou pare-feu entre les réseaux à protéger et l'extérieur.

II. L'architecture de sécurité

II.1 Contenu

Ce document décrit une architecture de sécurité définie afin de permettre une connectivité IP sécurisée, en recherchant le compromis entre souplesse d'utilisation et sécurité. Cette architecture est une base modulable en fonction des besoins et des spécificités de chaque site, de chaque organisation, et de chaque situation à laquelle elle doit être adaptée.

Cet architecture de sécurité est constituée des éléments suivants :

— Un **Garde-Barrière** (*Gatekeeper*), constitué au minimum (cf figure 1) :

- d'un routeur, appellé **Routeur Garde-Barrière** (*Gatekeeper Router*),
- d'une machine UNIX, appellée **Serveur Garde-Barrière** (*Gatekeeper Server*).

Le Garde-Barrière se place entre les réseaux à protéger et le monde extérieur.

— Un ensemble d'ordinateurs à protéger, connectés sur un réseau IP.
Afin de s'adapter à la réalité des sites, ceux-ci sont classés en deux catégories :

- ceux auquels il est possible de faire confiance, appelés **machines agréées**,
- ceux auquels il n'est pas possible de faire confiance, appelés **machines non-agréées**.

— Un logiciel, émulant les démons *telnetd* et *ftpd* classiques. Ce logiciel est dédié au Serveur Garde-Barrière et permet d'authentifier et d'identifier des utilisateurs.
A l'heure actuelle ce logiciel est contitué :

- d'un démon telnet spécifique, appelé *in.gk-telnetd*,
- d'un démon ftp spécifique, appelé *in.gk-ftpd*,

Le terme "*in.gk-*d*" est utilisé pour *internet gatekeeper daemons*.

— Un ensemble de documents, réécris et adaptés pour chaque organisation (cf figure 2) :

- Ce document d'introduction, décrivant l'architecture de sécurité proposée et si nécessaire les raisons de son choix, adapté à chaque situation.
- Un manuel des exigences de sécurité pour le Garde-Barrière.
- Un cahier de recettes pour le Garde-Barrière, permettant de valider les exigences.
- Un manuel des exigences de sécurité pour les machines agréées, avec des exigences générales et des exigences spécifiques au système d'exploitation UNIX/POSIX.
- Un cahier de recettes pour les machines agréées UNIX/POSIX.
- Et d'autre documents en fonction des sites, en particulier une reconnaissance de responsabilité pour les utilisateurs de machines agrées, un journal de bord pour le Garde-Barrière, etc.

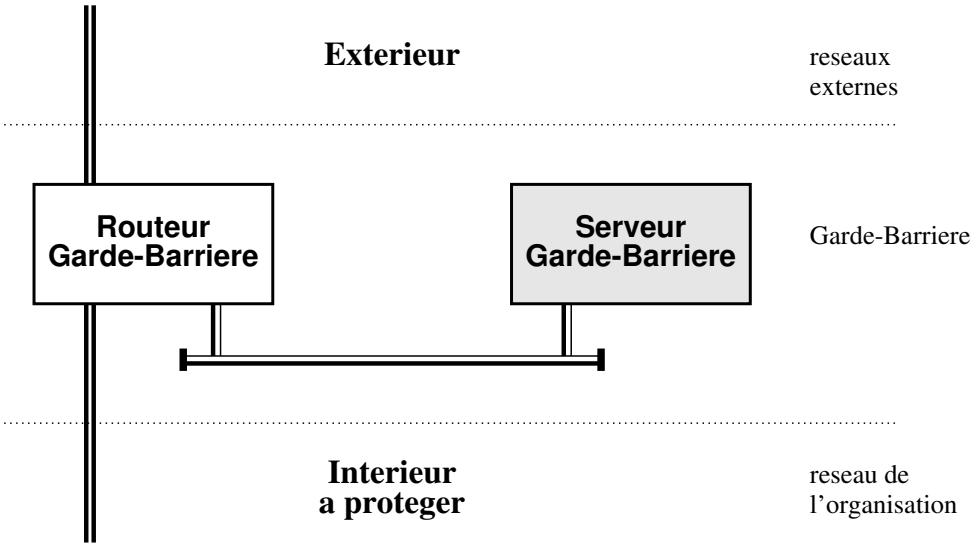

Figure 1. Architecture générale du Garde-Barrière

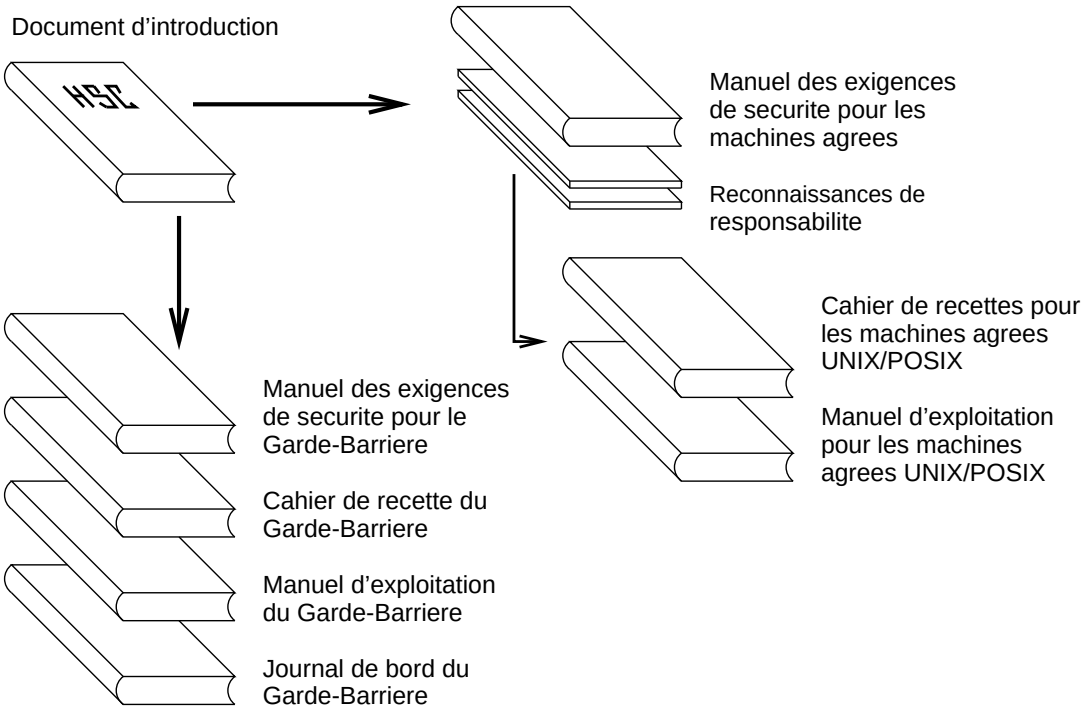

Figure 2. Organisation typique des documents

II.2 La démarche

Une réflexion de fond est nécessaire au préalable à la mise en place d'une connexion IP vers l'extérieur. Il est souhaitable de :

- Disposer d'une entité au sein de l'organisation, gérant de manière centralisée la sécurité, au moins à l'échelle de l'établissement ou de la division. Celle-ci dirige et relaye les fournisseurs, l'entité réalisant les agréments, le service responsable de l'exploitation du Garde-Barrière, etc.
- Définir et s'accorder sur la notion de site au sens géographique, et déterminer les zones de responsabilités et d'influence. Cela est indispensable pour obtenir une connectivité unique entre l'intérieur (le site géographiquement délimité), et l'extérieur (le reste).
- Procéder à une analyse, des risques apportés par la connectivité IP, en particulier vis-à-vis de la politique de sécurité de l'organisation si celle-ci existe. Cette analyse permet de déterminer les besoins de sécurité et de déterminer quelles solutions mettre en oeuvre pour minimiser ces risques. Celle-ci doit être de préférence réalisée en conservant une vue globale des problèmes, même s'il est parfois nécessaire de travailler sur le détail de solutions techniques. Il faut essayer d'inclure dans les démarches entreprises tous les éléments significatifs vis-à-vis de la sécurité, et ne pas se focaliser à l'excès sur un détail ou un autre, même s'il est techniquement passionnant.

Cette démarche est réalisée conjointement avec l'organisation qui souhaite mettre en place sa (ou une) politique de sécurité vis-à-vis de l'ouverture de réseaux TCP/IP.

Les besoins de sécurité sont ensuite traduits en solutions concrètes, exploitables par le service gérant la sécurité s'il existe, par les administrateurs système et réseaux de l'organisation, et l'ensemble des utilisateurs. Ces solutions définissent une architecture globale de la sécurité IP qui tente de répondre du mieux possibles aux besoins. Cette démarche aboutit à l'architecture de sécurité qui introduit le Garde-Barrière, le partage des systèmes informatiques en deux catégories, "agréés" (ceux auxquels on aura une certaine confiance) et "non-agréés", les manuels d'exigences de sécurité qui traduisent sous forme exploitable les besoins de sécurité, et un logiciel d'identification et d'authentification sur le Garde-Barrière.

II.3 Les machines agréées

Dans le cadre de cette architecture de sécurité ainsi définie, un utilisateur peut passer à travers le Garde-Barrière de deux façons :

1. Directement :
   - L'utilisateur est sur une machine agréée, donc située sur les réseaux intérieurs, locaux à l'organisation, et va se connecter vers l'extérieur, via un service agréé sur cette machine (cf figure 3).
   - L'utilisateur est quelque part sur un réseau extérieur, et va se connecter vers une machine agréée à l'intérieur de la zone protégée, en demandant un service agréé sur cette machine.

   Dans ces deux cas, le Routeur Garde-Barrière laisse passer la communication.

2. Indirectement :
   - L'utilisateur est sur une machine non-agréée, située sur les réseaux intérieurs, et va se connecter vers l'extérieur (cf figure 4).
   - L'utilisateur est quelque part sur un réseau extérieur, et demande une connexion vers une machine non-agréée à l'intérieur de la zone protégée.

   Dans ces deux cas, il n'est pas possible de faire confiance à l'identification et l'authentification de l'utilisateur réalisée sur la machine source ou destination, si cette

authentification existe. Aussi l'utilisateur doit s'identifier et s'authentifier sur le Serveur Garde-Barrière, à travers les services *in.gk-telnet* et *in.gk-ftp*.

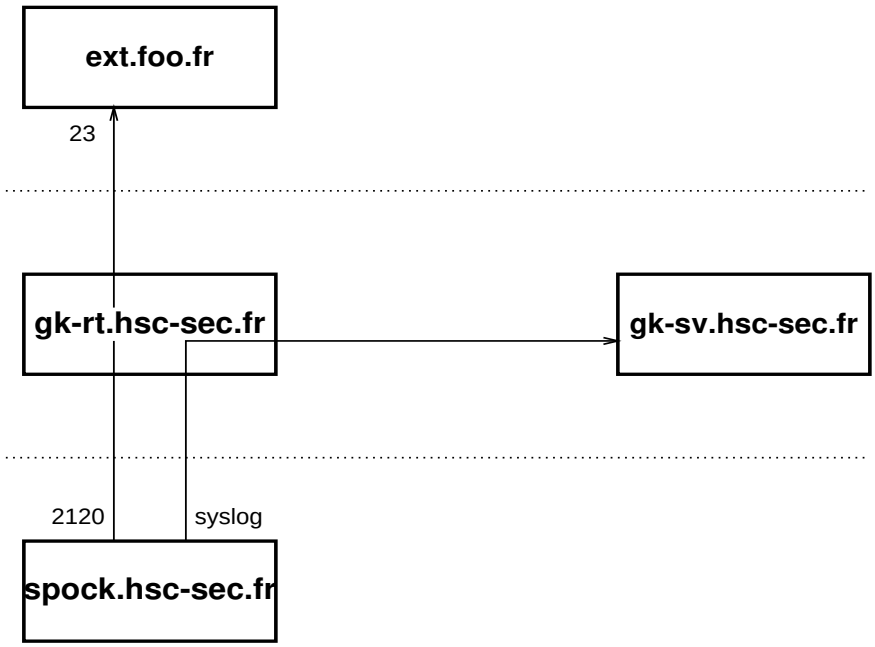

Figure 3. Connexion depuis une machine agréée vers l'extérieur

L'utilisateur se connecte de la machine *spock* vers la machine *ext* directement.

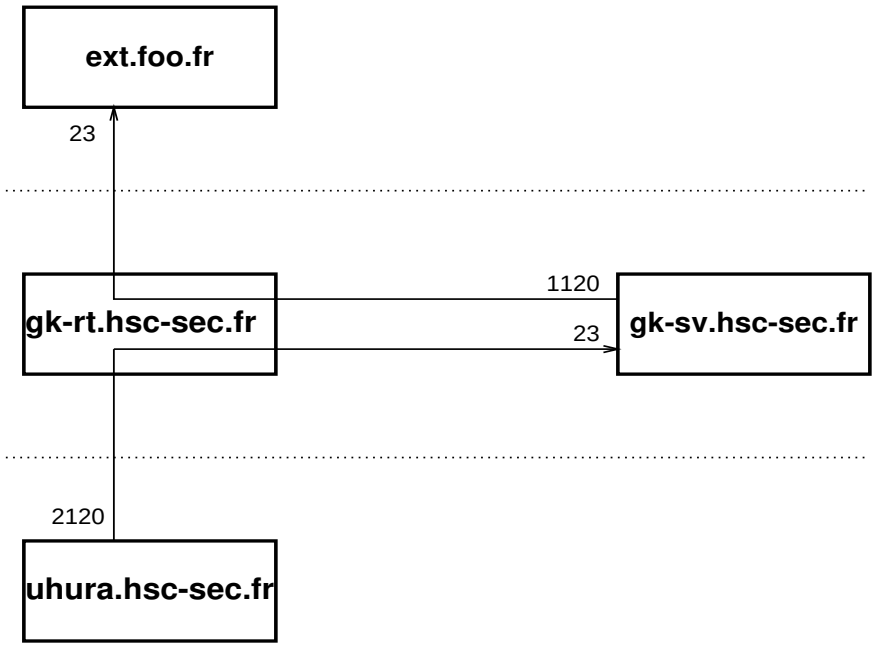

Figure 4. Connexion depuis une machine non-agréée via le serveur Garde-Barrière

L'utilisateur se connecte depuis la machine *uhura* vers le serveur Garde-Barrière *gk-sv* qui le relaye vers la machine *ext*.

La détermination de l'agrément d'une machine, pour devenir machine agréée, est basée sur le respect de règles d'administration strictes, qui concernent l'ensemble de la gestion et de l'exploitation de la machine. Ces règles s'adressent aux administrateurs et aux utilisateurs de cette machine. Celles-ci sont définies dans le manuel d'exigences de sécurité pour les machines agréées, elles permettent de formaliser la notion de confiance que l'on peut avoir dans une machine, et ainsi de permettrent a cette machine d'être ouverte à l'extérieur en minimisant les risques.

Cette distinction entre machines non-agréées, dont les utilisateurs doivent impérativement se servir du logiciel HSC-Gatekeeper d'identification et d'authentification sur le Garde-Barrière, et machines agréées, qui obtiennent un accès libre bien que contrôlé vers l'extérieur, est rendu indispensable dans la majorité des situations. Il apparait :

— que la culture et les habitudes des utilisateurs, ne permettent pas toujours la cassure, même transparente, de l'identification,

— que de nombreux services réseaux indispensables dans certains cas, ne permettent pas ou permettent difficilement une authentification au niveau utilisateur. Cela peut-être le cas des services suivants :

- Fenêtrage X11,
- Partage d'imprimantes `lpd`,
- Gestion de fichiers répartie NFS,
- Recherche de logiciels Archie,
- Discussion IRC,
- *Frame Buffer*,
- SGBD Client/Serveur,
- Applications avec des supercalculateurs.

Dans ces cas, seules les machines, ou les applications, pourront s'identifier et s'authentifier de machine à machine, ou à l'aide d'une tierce partie, mais avec une connectivité IP nécessairement directe, ne traversant que des routeurs.
Ce sont ces services, l'utilisation régulière des services TELNET et FTP, et l'adaptation à la culture Internet existante, qui imposent la notion de machine agréée.

Un service informatique central ou un service de sécurité est chargé de valider ou de faire valider les machines qui souhaitent bénéficier de l'agrément. Il veille à la validité de cet agrément dans le temps.

III. Le Garde-Barrière

III.1 Description

L'architecture de sécurité qui réponds aux besoins des utilisateurs introduit le Garde-Barrière. Le Garde-Barrière permet de connecter des réseaux IP entre une organisation, c'est-à-dire les **réseaux intérieurs**, et l'Internet ou d'autres réseaux, c'est-à-dire de manière plus générale les **réseaux extérieurs**. Il permet de le faire en répondant aux besoins des utilisateurs et en respectant la politique de sécurité que ceux-ci ont définie.

L'utilisation d'un tel Garde-Barrière répond aux besoins classiques des organisations souhaitant mettre en place des connexions IP avec de la sécurité. Ces connexions sont généralement vers l'Internet, mais peuvent être vers d'autres sites ou d'autres établissements, ou alors entre un réseau

classique et un réseau nécessitant une protection particulière, plus confidentiel par exemple.

III.2 Adaptabilité

L'architecture de sécurité basée sur l'utilisation du Garde-Barrière permet de s'adapter à l'ensemble des situations.
Elle tient compte :

- de la nécessité d'avoir des machines ayant un accès libre aux réseaux extérieurs : les machines agréées,
- du besoins des utilisateurs, qui même avec un PC (qui ne peut généralement pas être agréé) ou un compte sur une machine sans administrateur, peuvent tout de même utiliser FTP et TELNET vers l'extérieur avec un minimum de contraintes.

Ainsi les utilisateurs ne voient pas de suppressions de service ou de regression majeure des services fournis, à cause de la sécurité.

III.3 Constitution

Le Garde-Barrière est constitué :

- d'un routeur IP, muni de possibilité élaborées de filtrage IP. Plusieurs fournisseurs peuvent répondre à ce besoin. Le choix final intègrera, outre les besoins de sécurité, la culture d'entreprise.
- d'une machine UNIX, munie de capacités et de qualités réseaux et disques adéquat.

Ces deux éléments sont connectés entre eux par un réseau Ethernet local au Garde-Barrière. Comme indiqué en introduction le routeur est appellé Routeur Garde-Barrière et la machine UNIX Serveur Garde-Barrière.
Ces deux appareils peuvent être doublés, afin de garantir une meilleure sureté de fonctionnement, si les besoins de l'utilisateur le demandent.

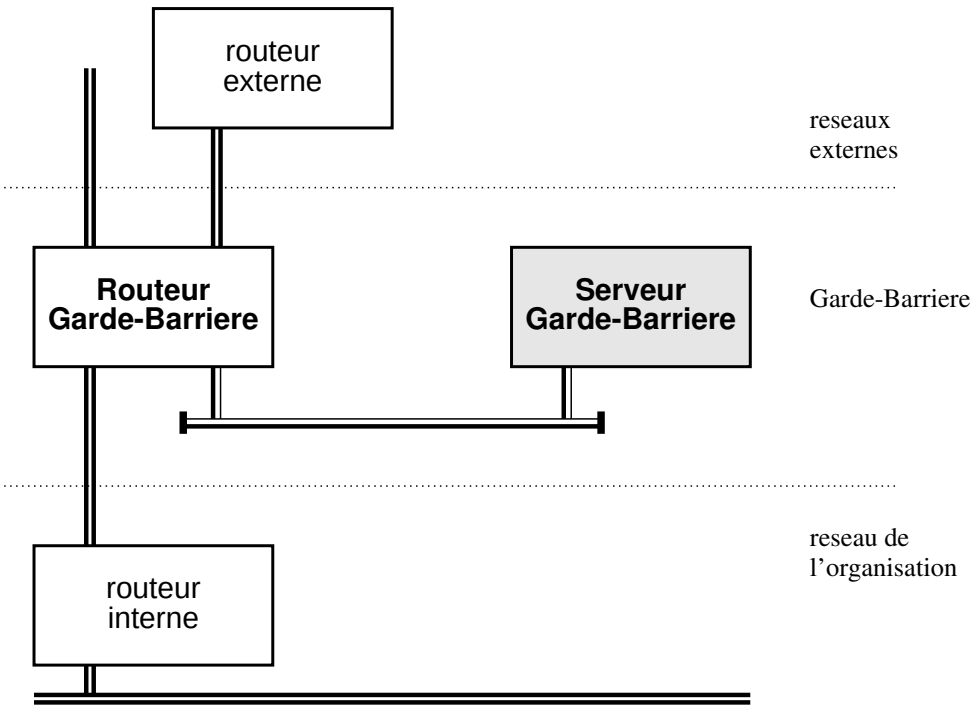

Figure 5. Architecture du Garde-Barrière

Les routeurs extérieurs et intérieurs ne sont pas utiles au Garde-Barrière, ils ne sont là qu'à titre d'exemples. Les réseaux intérieur et extérieur peuvent être directement branchés sur le Routeur Garde-Barrière.

III.4 Double protection

Le Garde-Barrière agit dans les deux sens :

- de l'extérieur vers l'intérieur
- de l'intérieur vers l'extérieur

La protection vis-à-vis de l'extérieur est la partie majeure de la sécurité, mais se prémunir contre les ennuis que d'autres organisations pourraient vous faire en vous accusant de leur avoir causé des problèmes, est aussi une partie à ne pas négliger. Le Garde-Barrière permet de gérer ces deux situations.

III.5 Pourquoi un tel Garde-Barrière ?

L'utilisation d'un Garde-Barrière tel que décrit ici est fondamentale. L'expérience montre qu'une organisation peut se retrouver connectée à l'Internet sans le savoir : un jour un service ou un département a besoin de la connectivité vers l'Internet, alors il s'en dote. Mais étant lui-même connecté aux réseaux de l'organisation, l'ensemble des machines se retrouvent connectées sans que les services centraux ou de sécurité ne le sachent. Cela est pour certains un important problème de sécurité. Aussi l'objectif du Garde-Barrière est de proposer aux utilisateurs une bonne connectivité IP, afin que ceux-ci ne soient pas tentés de mettre en place la leur, mais utilisent celle offerte par le Garde-Barrière.

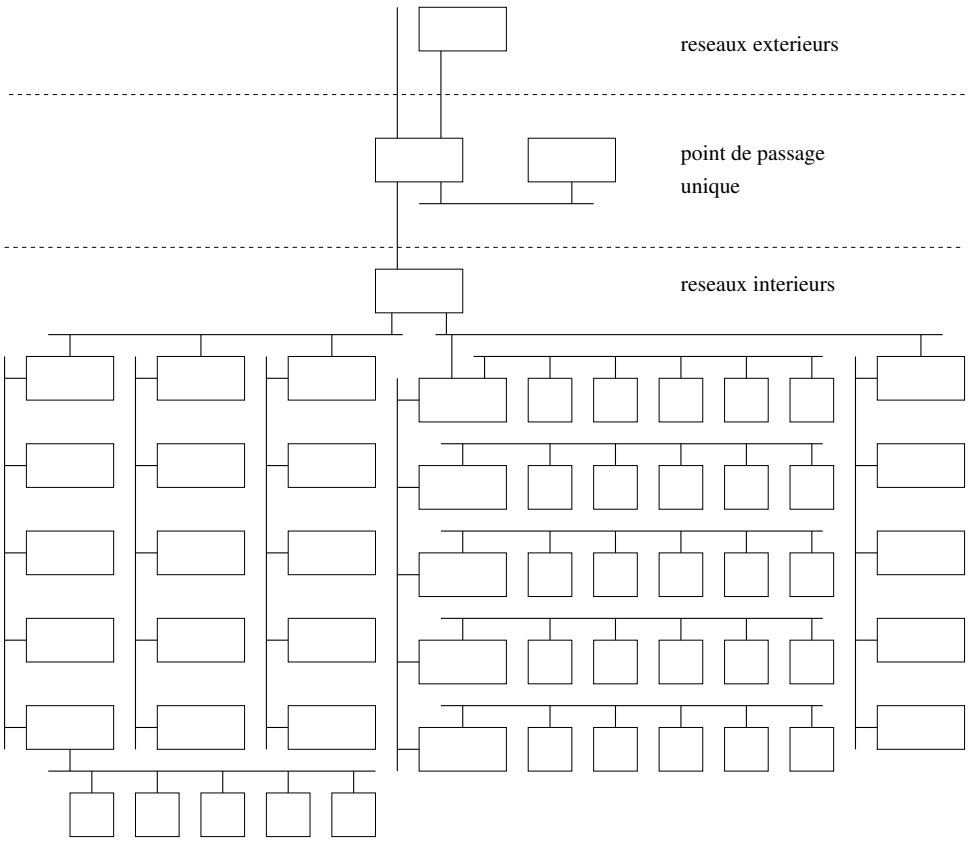

Figure 6. Point de passage unique entre intérieur et extérieur

Il est nécessaire à toute politique de sécurité, même simple, que la connectivité IP soit mise en place par un service centralisé et compétant, au service des utilisateurs de l'ensemble de l'organisation. Il n'est pas souhaitable que celle-ci soit mise en place par un département ou un laboratoire particulier, dont l'informatique n'est pas forcément le rôle. C'est pour réussir cette connectivité extérieure centralisée qu'il faut fournir des services de qualité aux utilisateurs.

De plus, c'est la mise en place d'un point unique de passage entre intérieur et extérieur qui permet de suivre une politique de sécurité plus sévère, avec des filtres sur les communications. C'est aussi la connectivité centralisée qui permet de n'autoriser que les services IP nécessaires, et de n'autoriser les communications que de machines et d'utilisateurs clairement identifiés.

III.6 Organisation géographique

Par ailleurs, l'expérience montre qu'il est préférable pour une connexion entre une organisation et l'Internet, de réduire cette connexion, entre un site géographiquement limité et le reste, y comprit l'Internet. Si une organisation dispose de plusieurs établissements, ceux-ci peuvent bénéficier du même garde-barrière vers l'Internet, mais doivent être considérés sur le site gérant le Garde-Barrière comme des réseaux extérieurs, et pas intérieurs. Ceci est préferable car dans la pratique, il est généralement difficile de disposer d'un contrôle réel sur un établissement, même de la même société ou de la même organisation, quand celui-ci est géographiquement éloigné.

Il en va de même pour les connexions des employés a partir de chez eux (en Dialup-IP par exemple), des connexions des partenaires, etc. Toute ligne spécialisée utilisée en IP doit être du coté extérieur, derrière le Garde-Barrière, et seuls les réseaux locaux doivent être sur le réseau intérieur.

Il faut ensuite pour avoir une politique cohérente pouvoir effectuer un minimum de contrôle sur l'intérieur, faire connaitre et promouvoir la politique de sécurité choisie, la diffuser, de manière a ce que les utilisateurs sachent d'une part qu'un service central leur offre la meilleure connectivité IP possible, et d'autre part qu'ils n'ont pas l'autorisation de mettre en place leur propre connectivité s'ils sont connectés aux réseaux internes.

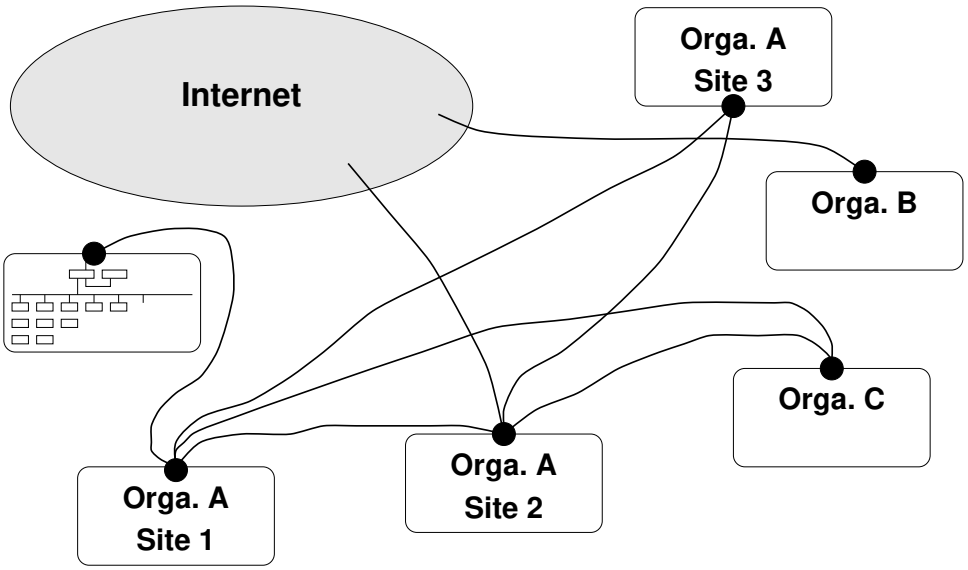

Figure 7. Délimitation géographique

III.7 Utilisation du Garde-Barrière

Dans le cadre de l'architecture de sécurité basée sur le Garde-Barrière, il a été vu que l'utilisateur peut passer à travers le Garde-Barrière de deux façons.

Dans le premier cas, l'utilisateur demande une communication de l'extérieur vers une machine agréée de l'intérieur, ou alors demande une communication de l'intérieur depuis une machine agréée vers l'extérieur. Dans ce cas le Routeur Garde-Barrière laisse passer la communication en ne filtrant pas les datagrammes IP, car le Garde-Barrière fait confiance à l'authentification et l'identification réalisée par la machine agréée.
Généralement, les services systématiquement ouverts aux machines agréées sont FTP et TELNET, mais sur certains sites, il n'y a pas de particularisme : un certain nombre de services sont interdits pour tous par le Routeur Garde-Barrière, tels que les services RPCs, et toutes les machines agréées peuvent utiliser les services autorisés. Dans d'autres cas, seuls les services demandés par les machines agréées sont autorisés.
Pour profiter de cette solution et être machine agréée, il faut avoir respecté les exigences décrites dans le manuel des exigences de sécurité pour les machines agréées, et avoir passé avec succès la recette permettant d'obtenir l'agrément.

Dans le second cas, l'utilisateur est contraint de passer par l'intermédiaire du Serveur Garde-Barrière. Il sera alors identifié et authentifié sur le Serveur Garde-Barrière.

Dans tous les cas, le Garde-Barrière doit suivre les exigences de sécurité pour le Garde-Barrière. La recette permettant de valider la sécurité du Garde-Barrière est passée par un service indépendant du service gérant la connectivité IP, tel que le service sécurité, ou par une société extérieure.

III.8 Services fournis

En résumé, le Garde-Barrière permet :

— de limiter les services sur TCP/IP entre l'intérieur et l'extérieur, en éliminant les services non-désirés,

— d'interdire l'accès aux sites indésirables,

— d'indiquer quelles sont les machines qui peuvent utiliser les services IP sans restriction (machines agréées), et de ne pas permettre aux autres machines de s'en servir,

— d'authentifier sur une machine nécessairement sûre (le Serveur Garde-Barrière), des utilisateurs souhaitant utiliser des services réseaux de ou vers des machines non-agréées,

— de filtrer les entrées et les sorties via le Serveur Garde-Barrière à partir de listes de contrôles d'accès sur le triplet (service, site, utilisateur),

— de contrôler l'utilisation des protocoles de routage,

— d'être passerelle pour le courrier électronique SMTP,

— d'être éventuellement passerelle pour les News,

— de journaliser un certain nombre d'éléments, connexions, utilisation de tel service, accès à telle machine, afin de suivre et contrôler l'exploitation du Garde-Barrière, et de permettre des enquêtes à postériori.

— de récupérer et analyser les informations de journalisation significatives vis-à-vis de la sécurité, fournies par le Routeur Garde-Barrière, les logiciels du Serveur Garde-Barrière, et des machines agréées si possible,

— de mettre en oeuvre une comptabilité de l'utilisation des services IP,

— de mettre en oeuvre un mécanisme de DNS interne/externe, afin de ne laisser transparaitre que les machines agréées vis-à-vis de l'extérieur,

— de gérer les correspondances adresses logiques IP/adresse physique Ethernet, pour tout ou partie des machines,

— de concentrer et contrôler de manière centralisée la connectivité IP.

III.9 Force et faiblesse du Garde-Barrière

Dans cette architecture de sécurité, il est nécessaire de bien réaliser que le Garde-Barrière et les machines agréées sont la force et la faiblesse du système. Le Garde-Barrière protège les réseaux et les machines intérieures, même si ceux-ci ne sont pas gérés correctement vis-à-vis de la sécurité ou pas administrés, mais si le Serveur Garde-Barrière est compromis, alors tout est compromis. De même, les machines agréées permettent d'utiliser des services Internet comme si le Garde-Barrière n'existait pas (du point de vue de l'utilisateur), mais si une machine agréée est compromise, c'est la porte ouverte à une attaque vers l'ensemble des machines non-agréées.

C'est pourquoi la sécurité et la résistance aux intrusions du Garde-Barrière et des machines agréées sont un élément capital de la réussite de l'architecture de sécurité. Une attention toute particulière doit être portée au Garde-Barrière et aux machines agréées, et au respect des exigences qui les concernent.

IV. Gestion des services applicatifs

IV.1 SMTP

Le protocole SMTP est le protocole de transport de courrier électronique sur l'Internet. Il est possible d'utiliser le Serveur Garde-Barrière comme passerelle de courrier électronique SMTP entre l'intérieur et l'extérieur de l'organisation. Mais il est aussi possible d'utiliser une machine agréée à l'intérieur. L'élément important est d'avoir un nombre de passerelles SMTP ayant la possibilité de recevoir du courrier de l'extérieur limité et déterminé. Ces passerelles serviront de relais pour l'ensemble des machines du réseau de l'organisation, en les protégeant. Les logiciels SMTP ne sont pas assez sûrs pour autoriser des connexions directes entre intérieur et extérieur pour tous les utilisateurs.

Même avec cette architecture, le protocole SMTP, dans sa version courante, reste non-sûr sur l'identification de l'utilisateur émetteur. Effet, on est obligé de partir du principe que l'on ne peut pas faire confiance à l'authentification de l'émetteur sur sa machine d'envoi de courrier. Mais il n'y a plus de risques d'intrusion.

Il est possible de mettre en place un contrôle strict et complet sur l'utilisation du courrier électronique. Un logiciel de filtrage du courrier électronique, sur le couple émetteur/destinataire, peut s'installer en ajout au logiciel de transfert du courrier Sendmail.

IV.2 NNTP

Le protocole NNTP est le protocole de transport des News (conférences réparties) sur les réseaux IP. Celui-ci ne comporte pas à priori de risques majeurs vis-à-vis de la sécurité. Il peut être géré à travers le Serveur Garde-Barrière, ou à travers un ou plusieurs serveurs agréés à l'intérieur de l'organisation, qui seront autorisés par le Routeur Garde-Barrière à recevoir et/ou à emettre des connexions NNTP vers l'extérieur.

La mise en place d'un serveur de News primaire centralisé pour l'organisation est généralement indispensable.

IV.3 FTP

Le service FTP peut-être accessible en entrée, comme en sortie, de deux manières :

— Directement dans le cas d'une machine agréée : Accès direct

— Indirectement dans le cas d'une machine non-agréée : Accès indirect
Dans ce cas l'identification et l'authentification de l'utilisateur sont réalisés sur le Serveur Garde-Barrière (cf Chapitre 7).

IV.3.1 Accès direct

L'utilisateur est sur machine agréée ou accède directement à une machine agréée de l'extérieur. L'administration de cette machine est soumise à l'éprreuve d'agrément d'une entité de contrôle centralisée, afin d'être machine agréée. Le Routeur du Garde-Barrière autorise les connexions FTP de l'extérieur vers cette machine ou depuis cette machine vers l'extérieur.

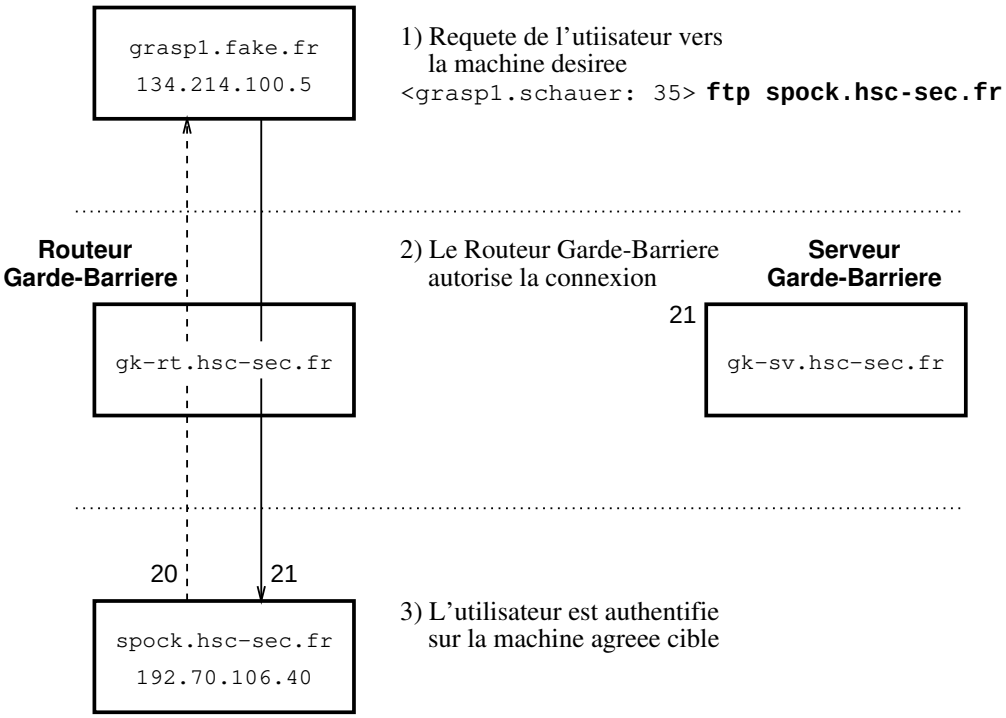

Figure 8. Connexion FTP en accès direct

IV.3.2 Accès indirect, via le Serveur du Garde-Barrière

L'utilisateur demande à accéder au Serveur Garde-Barrière, pour s'identifier et s'authentifier. Sur celui-ci il indique la machine de destination, et sa communication est automatiquement relayée de manière transparente.

Aucune modification des applications FTP clientes ou serveur sur les machines de départ et d'arrivée n'est nécessaire.

La figure suivante montre comment la connexion FTP à travers le Serveur Garde-Barrière est réalisée :

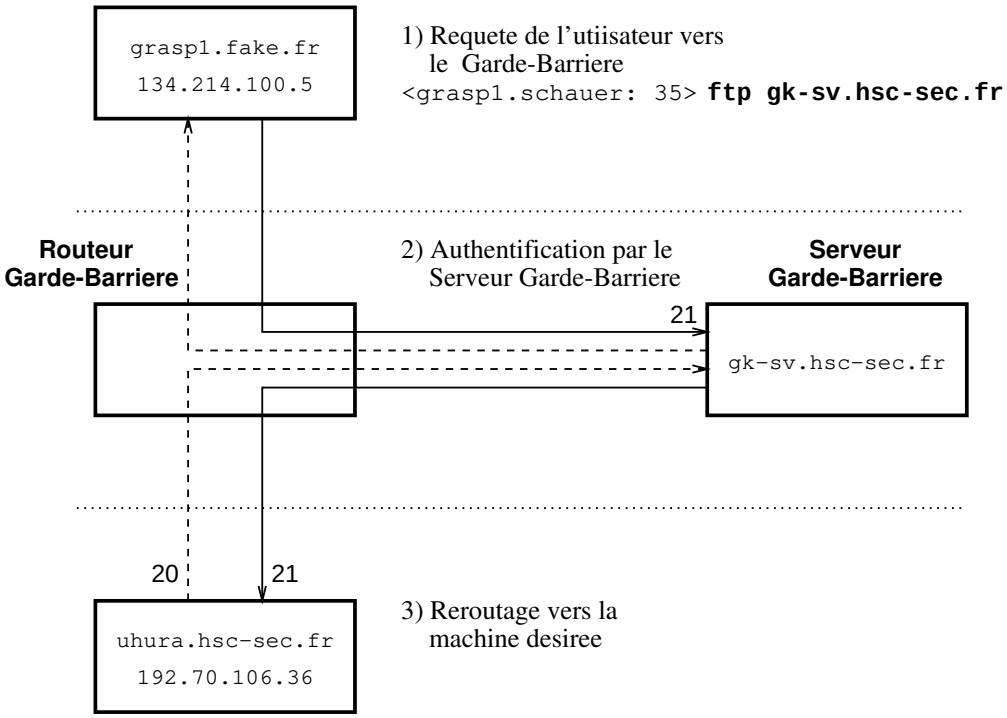

Figure 9. Connexion FTP à travers le Serveur Garde-Barrière

Les flèches indiquent le sens d'établissement de la session, pas le sens des transferts de données.

IV.4 TELNET

De même que pour le service FTP, le service TELNET peut-être utilisé de deux manières :

— Directement dans le cas d'une machine agréée.

— Indirectement dans le cas d'une machine non-agréée.
Dans ce cas l'identification et l'authentification de l'utilisateur sont réalisés sur le Serveur Garde-Barrière (cf Chapitre 7).

Les shémas de connexions pour le service TELNET sont les même que pour le service FTP.

IV.5 Journalisation

La journalisation est un service disponible sur UNIX, fourni par le démon `syslogd`. C'est un service local, qui permet cependant d'envoyer des données de journalisation vers une autre machine.
Dans l'architecture de sécurité du Garde-Barrière HSC, le service de journalisation est utilisé sur le Serveur Garde-Barrière pour gérer les informations significatives vis-à-vis de sa politique de sécurité. D'autres machines peuvent participer à l'exploitation et au traitement de ces données de journalisation.

La journalisation centralisée sur le Serveur Garde-Barrière, est produite par :

- les applications du Serveur Garde-Barrière, en particulier les démons serveurs qui authentifient et relayent les communications,
- le Routeur Garde-Barrière,
- des applications gérées de manière centralisée, situées hors du Garde-Barrière (cas possible du service de courrier électronique par exemple),
- les services réseaux des machines agréées.

IV.6 Serveur de noms

Le service de serveurs de noms est indispensable dans le cas d'une connexion Internet, par exemple pour authentifier les appels entrants. Il pourra être géré sur des machines (primaire et secondaire) intégrées au réseau du Garde-Barrière.

Il est aussi possible de mettre en place un serveur de noms externe, qui ne fera apparaitre vis-à-vis des réseaux extérieurs que les machine souhaitées (normalement des machines agréées), et un serveur de noms interne aux réseaux à protéger, qui fera apparaître vis-à-vis du réseau interne un serveur de noms normal.

IV.7 Routage IP

Un routage dynamique pourra être utilisé vis-à-vis des réseaux extérieurs, en particulier afin de faire jouer la redondance des lignes. Par contre, il est généralement préférable de mettre en place au sein d'un site géographique un cablage des réseaux en étoile, indépendamment de leur topologie. Celui-ci permet d'utiliser un routage statique, à moins que des redondances internes au site soient nécessaires.

IV.8 Autres services

La gestion des autres services est régentée dans les manuels d'exigences, en fonction des besoins de chaque site.

V. Exigences de sécurité pour le Garde-Barrière

L'architecture de sécurité comprend deux manuels fondamentaux qui définissent les exigences que doivent suivre le Garde-Barrière d'une part et les machines agréées d'autre part.
Chacun d'entre eux est complété par un cahier de recettes qui permet de valider le respect des exigences.

Le premier manuel d'exigences est destiné à formaliser la sécurité et la protection du Garde-Barrière. Celui-ci va permettre de valider l'administration et l'exploitation du Garde-Barrière vis-à-vis de la politique de sécurité.

Le manuel des exigences de sécurité pour le Garde-Barrière regroupe un peu plus de 300 exigences, qui concernent à la fois le Serveur Garde-Barrière et le Routeur Garde-Barrière. Ces exigences sont de trois types :

— des exigences à caractère obligatoire

— des recommendations à caractère facultatif,

— des informations ou des réactions à suivre en cas d'incident.

Ces dernières sont des exigences à caractère informatif, qui soit sont indispensables en amont des véritables exigences et recommendations, soit qui seront à suivre dans la mesure du possible en cas d'incident.

Toutes les exigences sont applicables au Garde-Barrière tel qu'il est utilisé en exploitation dans l'organisation cible. Le manuel doit être adapté en fonction du type de matériel utilisé, en particulier les différents fournisseurs de routeurs gèrent de manière très différente le filtrage IP.

Les exigences et recommendations du manuel concernent :

- la protection et le contrôle d'accès à l'ensemble du Garde-Barrière,
- la qualité des administrateurs système et réseaux du Garde-Barrière,
- l'administration et la gestion du Serveur Garde-Barrière,
- la protection et le contrôle d'accès réseau sur le Serveur Garde-Barrière, en détaillant les exigences pour chaque service réseau : DNS, équivalences, routage IP, TFTP avec le Routeur Garde-Barrière, la passerelle de courrier électronique SMTP, l'utilisation de X11 sur le réseau du Garde-Barrière, SNMP, les services d'identification et d'authentification pour TELNET et FTP (par `in.gk-telnetd` et `in.gk-ftpd`), etc,
- l'administration et la gestion du Routeur Garde-Barrière,
- le filtrage IP et sa gestion sur le Routeur Garde-Barrière,
- la journalisation et la comptabilité des utilisations du Garde-Barrière,
- la gestion des incidents et la reconfiguration du Garde-Barrière,
- la sauvegarde et l'archivage.

Le manuel des exigences de sécurité pour le Garde-Barrière est complété par un cahier de recettes, en partie spécifique à chaque implantation. Celui-ci reprend chaque exigence par son numéro, et propose des tests sous forme de recettes utilisables durant l'exploitation du Garde-Barrière, permettant de vérifier le suivi de l'exigence.

Pour chaque recette, il est indiqué quels appareils du Garde-Barrière elle concerne, dans quel cas il faut l'utiliser, avec quelle fréquence, le résultat prévisible, et les actions à mener en fonction du résultat. L'objectif est de pouvoir faciliter le suivi des exigences du Garde-Barrière par ses administrateurs, et leur vérification par l'entité de contrôle (le service de sécurité ou tout autre service adéquat).

VI. Exigences de sécurité pour les machines agréées

Les exigences pour les machines agréées permettent de déterminer dans quel cadre les utilisateurs d'une machine, ou d'un ensemble de machines d'un réseau, peuvent utiliser des services vers l'extérieur ou depuis l'extérieur, sans utiliser l'identification et l'authentification du Serveur Garde-Barrière. Lorsque qu'une machine a obtenu l'agrément, celle-ci devient une machine agréée. Le Garde-Barrière fait confiance à cette machine, c'est-à-dire qu'il fait confiance à l'identification et l'authentification des utilisateurs sur cette machine et à la qualité de son administration.

Le manuel des exigences de sécurité pour les serveurs agréés regroupe un peu plus de 150 exigences, rangées par chapitres. Ces exigences sont de deux types :

- exigences (*requirements*),
- recommandations (*guidelines*).

Une exigence doit être impérativement suivie, elle a un caractère obligatoire. Une recommendation doit être suivie dans la mesure du possible, elle n'est pas obligatoire mais recommandée.

De plus chaque exigence appartient une classe. Deux classes sont déjà utilisées :

- les exigences génériques,
- les exigences spécifiques à UNIX.

Les exigences génériques sont des exigences valables à priori sur n'importe quel système d'exploitation. Celles-ci sont parfois précisées dans leur application sur UNIX, lorsque cela est utile. Par exemple une exigence sur la manière de choisir un bon mot de passe est générique. Les exigences spécifiques à UNIX concernent des aspects plus précis, comme la configuration des fichiers `/etc/exports` ou `/etc/dfs/dfstab` pour NFS. Toutes les exigences sont applicables à UNIX, et la moitié d'entre-elles lui sont spécifiques.

Les exigences et recommandations du manuel concernent :

- les administrateurs, par exemple concernant leur formation,
- les utilisateurs, par exemple concernant leurs responsabilités,
- le contrôle d'accès physique de la machine agréée, par exemple concernant l'utilisation de mots de passes sur la PROM d'amorçage,
- l'identification et l'authentification des utilisateurs, par exemple concernant l'usage de mauvais mot de passes,
- la gestion des sessions des utilisateurs, par exemple concernant le `PATH` ou `/dev/kbd`.
- la gestion des comptes d'administration (les comptes de type *root*, avec un UID égal à 0), par exemple sur le partage de mots de passes sur ce type de compte,
- la gestion des permissions des fichiers et répertoires sur le système de gestion de fichiers, par exemple les permissions des répertoires temporaires,
- la gestion des utilisateurs par les administrateurs, par exemple les démarches à entreprendre auprès d'un utilisateur qui persiste à utiliser un mauvais mot de passe,
- la gestion de la journalisation et de la comptabilité, par exemple ce qu'il faut faire des jounaux,

- l'organisation générale, par exemple concernant les changements qui doivent être signalés au service d'agrément,
- le contrôle d'accès et l'identification du serveur agréé, par exemple concernant l'utilisation de noms de machines complètement qualifiés,
- les services réseaux, chaque service est detaillé : TELNET, FTP, SENDMAIL, NFS, NIS, X11, DNS, etc. Cette partie est la plus conséquente.

Le manuel des exigences de sécurité pour les machiness agréées est complété par un cahier de recettes. Celui-ci reprend chaque exigence par son numéro, et propose des solutions permettant de vérifier le suivi de l'exigence.

Pour chaque recette, il est indiqué à qui elle est destinée, dans quel cas il faut l'utiliser, avec quelle fréquence, en test ou en exploitation, le résultat prévisible, et les actions à mener en fonction du résultat, sans être exhaustif. L'objectif est de faciliter le travail des administrateurs et des auditeurs réalisant les agréments et leur suivi. Dans certains cas, la solution est simple, lorsqu'il suffit d'utiliser COPS par exemple, mais dans d'autres cas il faut envisager des vérifications sur le terrain, c'est le cas pour une exigence qui demande aux utilisateurs de verrouiller leur écran (par `xlock` par exemple) avant de quitter son poste de travail.

Dans certains cas, l'utilisation de logiciels complémentaires au système d'exploitation est nécessaire au respect des exigences ou à leur recette. Cela peutêtre le cas de logiciels tels que ARM/ASET sur Sun, ou de logiciels d'aide à la sécurité issus du domaine public (c'est-à-dire distribués gratuitement et librement) tels que COPS, *lock*, *xnlock*, *xsecure*, *tcp_wrapper*, *ftpd-logging*, etc.

VII. Identification et authentification sur le Garde-Barrière

VII.1 Fonctionnement

Quand un canal de communication à besoin d'être établi vers ou depuis une machine non-agréée, l'utilisateur est obligé d'utiliser les services du Serveur Garde-Barrière. Deux services fondamentaux sont actuellement proposés : FTP et TELNET. L'identification et l'authentification est réalisée par le remplacement de `ftpd` et `telnetd` par des nouveaux démons. Il n'y a aucun compte utilisateur sur le Serveur Garde-Barrière.

Ces nouveaux démons, nommés `in.gk-telnetd` et `in.gk-ftpd`, sont appelés par `inetd` en remplacement des anciens démons `in.telnetd` et `in.ftpd`. Si `inetd` n'est pas considéré comme sûr, il est possible de modifier le code des nouveaux démons pour leur faire gérer leur canaux respectifs.

D'autres services pourront intégrer ce type d'identification et d'authentification à l'avenir, toute étude est possible.

Les deux serveurs implantés (TELNET et FTP), assurent l'identification et l'authentification de l'appelant. En cas d'identification incorrecte (mauvais nom d'utilisateur) ou d'authentification incorrecte (erreur de mot de passe), l'accès au service est bien entendu refusé. Ensuite l'adresse source, et l'adresse destination demandée, sont vérifiées vis-à-vis des tables de contrôle. La source et la destination doivent toutes les deux être autorisées pour cet utilisateur afin de permettre l'utilisation du relayage (ou reroutage IP) par *in.telnetd* ou *in.ftpd*.
Le Routeur Garde-Barrière garantit, que excepté sur les machines agréées, aucun utilisateur ne peut le traverser. L'utilisateur doit se connecter sur le Serveur Garde-Barrière.

Tous les évènement gérés par `in.gk-telnetd` et `in.gk-ftpd` sont journalisés à travers le service *syslog*.

Voici des exemples de sessions et de la journalisation associée, issue de *syslog* :

```
<hsc.schauer: 63> telnet gk-sv.hsc-sec.fr
Trying...
Connected to gk-sv.hsc-sec.fr.
Escape character is '^]'.

gk-sv.hsc-sec.fr

login: schauer
Password: mot_de_passe_sur_le_Serveur_Garde-Barrière
Host: itesec.hsc-sec.fr

Access authorized

UNIX(r) System V Release 4.0 (itesec)

login: schauer
Password: mot_de_passe_sur_la_destination_finale
UNIX System V Release 4.0 AT&T NEWS3400
itesec
Copyright (c) 1984, 1986, 1987, 1988 AT&T
All Rights Reserved
Last login: Mon Jul 13 11:56:28 from spock.hsc-sec.fr
<itesec.schauer: 346>
```

Les évènements suivants sont envoyés au service *syslog*, en utilisant les abbréviations suivantes :

sa adresse source (*source address*).

u utilisateur identifié, ou "_UNKNOWN" s'il n'est pas dans la base de données.

pt n° de séquence des essais de mot de passe (*password tries*), qui débute à chaque nouvelle session.

pc drapeau indiquant si le mot de passe a été changé (1) ou pas (0) (*password change*). Le changement de mot de passe n'est disponible qu'avec le service TELNET.

da adresse destination, si elle est connue, "_NOHOST" sinon (*destination address*).

La dernière partie de la ligne contient les messages indiquant l'état de la connexion. Les entrées présentées ci-dessous ont été imprimées en deux lignes pour permettre la lecture, mais celle-ci sont sur une ligne dans la réalité.

```
Jul 21 14:27:45 gk unix: Jul 21 14:27:45 gk-telnetd[10716]:
sa=192.70.106.33 u=schauer pt=1 pc=0 da=itesec.hsc-sec.fr start of session
[...]
Jul 21 14:27:45 gk unix: Jul 21 14:37:45 gk-telnetd[10716]:
sa=192.70.106.33 u=schauer pt=1 pc=0 da=itesec.hsc-sec.fr end of session
```

Exemples de connexions échouées au niveau de l'identification/authentification :

```
<hsc.wolf: 71> telnet gk-sv.hsc-sec.fr
Connected to gk-sv.hsc-sec.fr.
Escape character is '^]'.

gk-sv.hsc-sec.fr

login: wolf
Password: un_mauvais_mot_de_passe
Login incorrect
login: schauer
Password: un_autre_mauvais_mot_de_passe
Login incorrect
login: notwolf
Password: last_but_not_least
Login incorrect
Connection closed by foreign host.
```

Après trois erreurs (configuration par défaut), la session est fermée. Le service *syslog* reporte les tentatives d'accès, et le compteur *pt* est incrémenté jusqu'a trois :

```
May  6 14:31:42 gk unix: May  6 14:31:42 gk-telnetd[10778]:
sa=192.70.106.33 u=wolf pt=1 pc=0 da=_NOHOST bad password
May  6 14:31:42 gk unix: May  6 14:31:47 gk-telnetd[10778]:
sa=192.70.106.33 u=schauer pt=2 pc=0 da=_NOHOST bad password
May  6 14:31:42 gk unix: May  6 14:31:59 gk-telnetd[10778]:
sa=192.70.106.33 u=_UNKNOWN pt=3 pc=0 da=_NOHOST bad password
```

Un utilisateur peut aussi être validé au niveau de l'identification et de l'authentification, mais demander une machine vers laquelle il n'a pas le droit d'aller :

```
<hsc.wolf: 78> telnet gk-sv.hsc-sec.fr
Connected to gk-sv.hsc-sec.fr.
Escape character is '^]'.

gk-sv.hsc-sec.fr

login: wolf
Password: mot_de_passe_de_wolf
Host: 134.135.136.137
Unauthorized destination.
[...]


May  6 14:35:57 gk unix: May  6 14:35:57 gk-telnetd[10790]:
sa=192.70.106.33 u=wolf pt=1 pc=0 da=134.135.136.137 destination address rejected
[...]
```

Le comportement du serveur FTP est similaire, mais bien entendu l'interface est complètement différente :

```
<hsc.schauer: 56> ftp gk-sv.hsc-sec.fr
Connected to gk-sv.hsc-sec.fr.
220- gk-sv.hsc-sec.fr FTP server / HSC ready.
     After logging in, use 'site machine' to connect
     to the desired machine.
220  Time is 1992/07/24 16:48:21 GMT
Name (gk-sv:schauer): schauer
331 Password required for schauer.
Password: mot_de_passe_sur_le_serveur_Garde-Barrière
230 User schauer logged in. Please select your host.
Remote system type is UNIX.
ftp> site kirk.hsc-sec.fr
220 kirk FTP server (NCC-1701) ready.
ftp> user schauer
331 Password required for schauer.
Password: mot_de_passe_sur_la_machine_kirk
230 Welcome on board Captain schauer.
ftp>
```

Le service *syslog* reporte les lignes suivantes. Le champs *pc* est conservé mais n'a pas de signification car le changement de mot de passe n'est pas implanté dans le serveur FTP.

```
Jul 24 14:47:45 gk unix: Jul 24 14:47:45 gk-ftpd[14302]:
sa=192.70.106.33 u=schauer pt=1 pc=0 da=kirk.hsc-sec.fr start of session
[...]
Jul 24 14:47:45 gk unix: Jul 24 14:57:40 gk-ftpd[14302]:
sa=192.70.106.33 u=schauer pt=1 pc=0 da=kirk.hsc-sec.fr end of session
```

Avec des destinations interdites :

```
<hsc.schauer: 63> ftp gk-sv.hsc-sec.fr
Connected to gk-sv.hsc-sec.fr.
220- gk-sv.hsc-sec.fr FTP server / HSC ready.
     After logging in, use 'site machine' to connect
     to the desired machine.
220  Time is 1992/05/06 14:32:21 GMT
Name (gk-sv:schauer): schauer
331 Password required for schauer.
Password: mot_de_passe_sur_le_serveur_garde-barriere
230 User schauer logged in. Please select your host.
Remote system type is UNIX.
ftp> site 134.135.136.137
550 You are not authorized to call 134.135.136.137.
ftp> site 134.135.136.138
550 You are not authorized to call 134.135.136.138.
ftp> site 134.135.136.139
221-You are not authorized to call 134.135.136.139.
221 Goodbye. Thanks for using HSC products.
ftp>
```

Le journal de *syslog* contient :

```
May  6 14:35:57 gk unix: May  6 14:35:57 gk-ftpd[10790]:
sa=192.70.106.33 u=schauer pt=1 pc=0 da=134.135.136.137 destination address rejected
May  6 14:35:57 gk unix: May  6 14:36:27 gk-ftpd[10790]:
sa=192.70.106.33 u=schauer pt=1 pc=0 da=134.135.136.138 destination address rejected
May  6 14:35:57 gk unix: May  6 14:36:57 gk-ftpd[10790]:
sa=192.70.106.33 u=schauer pt=1 pc=0 da=134.135.136.139 destination address rejected
```

VII.2 Configuration

La configuration du service d'identification et d'authentification pour les deux démons utilise trois tables :

— un fichier de type *passwd* des utilisateur et de leurs mots de passes,

— un fichier de type *group* pour le filtrage des adresses sources,

— un fichier de type *group* pour le filtrage des adresses destinations,

Tous ces fichiers doivent être manipulés avec la même prudence que les fichier `/etc/passwd` et `/etc/group` originaux, car ils contiennent des informations vitales.

Le fichier des mots de passe est un fichier *passwd* classique d'UNIX, allégé, c'est-à-dire qu'il a le même nombre de champs, mais certains d'entre eux ne sont pas utilisés. Les champs utilisés pour le moment sont les champs *login* et *password*. Les autres peuvent contenir ou pas des informations. L'identification et l'authentification pour les services TELNET et FTP est basée sur ce fichier.

```
wolf:1234567890123:::Christophe Wolfhugel::
schauer:2345678901234:::Herve Schauer::
```

Les fichiers de filtrage ont la même syntaxe que le fichier `/etc/group` classique d'UNIX, sauf que la plupart des champs ont changé de signification afin de s'adapter à nos besoins :

```
134.214.0.0:255.255.0.0::wolf
192.70.106.0:255.255.255.0::schauer,wolf
192.70.107.1::schauer
```

Le premier champ correspond à l'adresse réseau qui est autorisée et le second champ au masque réseau à appliquer. Un masque de 0.0.0.0 autorise toutes les adresses, alors que 255.255.255.255 donne accès seulement à la machine adressée dans le premier champ. Le dernier champ est la liste des utilisateurs autorisés. Pour résumer : on applique un "et" logique entre l'adresse IP (source/destination) et le masque. Si le résultat est le réseau indiqué la source/destination est validée, sinon elle est rejetée.

En prenant pour exemple le fichier précédent comme table de contrôle des adresses source, la première ligne permet à l'utilisateur *wolf* d'appeler de n'importe quelle machine du réseau 134.214, la seconde permet à *schauer* et *wolf* de se connecter depuis le réseau 192.70.106, et la dernière permet seulement à *schauer* d'appeler depuis la machine 192.70.107.1.

Le fichier des adresses destination est utilisé pour la même vérification vis-à-vis de la machine demandée, une fois que l'utilisateur a été identifié avec succès et que sa machine source est autorisée.

```
192.70.106.0:255.255.255.252::wolf,schauer
```

Dans cet exemple les utilisateurs *wolf* et *schauer* sont autorisés à se connecter sur les machines .1, .2, .3 (masque en .252, il reste les 2 derniers bits de libre) du réseau 192.70.106.

Les formats standard de fichiers UNIX sont utilisés car l'implémentation peut ainsi utiliser les appels système et fonctions de bibliothèque UNIX standard pour y acceder, y comprit `crypt()` pour le chiffrement des mots de passes.

L'identification et l'authentification sur le Serveur Garde-Barrière à travers les services TELNET et FTP est totalement transparente. Celle-ci est complètement conforme aux RFCs et ne demande aucune modification des logiciels TELNET ou FTP sur les machines client ou serveur.
L'identification réalisée dans les exemples utilise le même principe que le *login/passwd* d'UNIX/POSIX, mais une authentification à base de calculette DES (*Smart Card*, *SecureNetKey*, etc) ou carte à puce est possible.

VIII. Conclusion

VIII.1 Organisation à mettre en oeuvre

Afin d'aboutir à une mise en oeuvre réussie de l'architecture de sécurité proposée, il est nécessaire de bien penser à l'organisation indispensable autour de sa mise en place. Il ne suffit pas d'installer `in.gk-ftpd`, de donner le manuel des exigences du Garde-Barrière aux administrateurs de celui-ci, et de se précipiter à faire passer la recette...

La sécurité est un tout, c'est pourquoi il faut essayer de voir les choses de manière globale et penser à l'avance à la répartiton des tâches, à la recherche et la formation des ressources humaines, à la mise en place du service technique d'agrément, aux autorités compétentes en cas de conflits, à la déclaration des adresses IP auprès du NIC, etc.

Il faut tout particulièrement penser à l'information et à la sensibilisation des utilisateurs. Ils sont les premiers concernés et c'est pour la sécurité de leur travail qu'une telle passerelle est mise en place. Il faut cependant les persuader que la politique de sécurité n'est pas là pour les gêner mais pour défendre leurs intérêts. C'est pourquoi une information et une concertation générale, réalisée dès le départ de l'action, et impliquant l'ensemble du personnel, est souhaitable.

Enfin il ne faut pas se précipiter à se brancher sur l'Internet si on ne l'était pas. Une période de tests permettant de roder l'exploitation du Garde-Barrière est souhaitable. Durant cette période, le véritable réseau intérieur de l'organisation ne sera pas branché sur le Garde-Barrière, mais une ou deux machines faisant office de leurres y prendront place. Cette période peut être mise à profit pour agréer les machines des services ayant des besoins urgents de connectivité IP, qui seront autorisées à utiliser les services IP vers l'extérieur dès la mise en exploitation du Garde-Barrière.

VIII.2 Conclusion

Les besoins d'ouverture et de connectivité ne cessent de se développer dans toutes les organisations. Parallèlement, les besoins de sécurité se font de plus en plus sentir. Ces deux nécessités ne sont pas contradictoires, l'architecture de sécurité basée sur le Garde-Barrière permet d'adapter à chacun le juste milieu qui permet de les concilier.