

Passerelles Internet Sécurisées

par
Hervé Schauer



Hervé Schauer Consultants
Securicom 94

Passerelles Internet Sécurisées

par
Hervé Schauer

Email: Herve.Schauer@hsc.fr.net

Télécopie: +33 (1) 46 38 05 05

Téléphone: +33 (1) 46 38 89 90

2 Juin 1994

La composition de ce document a été entièrement réalisée sur le système d'exploitation Unix, à l'aide :

- du formateur de document standard *troff*, accompagné des filtres standards *pic*, *tbl* et *eqn*,
- du filtre *accent* de Philippe Dax (ENST),
- du logiciel de dessin *xfig*, et des filtres *fig2dev* et *psfig*,
- du prévisualiseur *Ghostscript*,
- du traducteur PostScript *tscript* de Gilles Dauphin (ENST).

Copyright © Hervé Schauer Consultants 1989, 1990, 1991, 1992, 1993, 1994
Reproduction strictement interdite

Passerelles Internet

- 1. Modèles possibles de passerelles TCP/IP**
- 2. Le filtrage IP**
- 3. Les routeurs**
- 4. Le relayage de services**
- 5. Les cartes et calculettes**
- 6. Le rôle des CERTs**

I. Modèles possibles de passerelles TCP/IP

- Pas de connexion
- Une connexion sans rien
- Une machine ou un boitier
- Un routeur
- Une combinaison d'un routeur et d'une machine

II. Le filtrage IP

- La base de la sécurité réseau

- Réalisé par un ou plusieurs routeurs :
 - protège et contrôle tout ou partie du réseau
 - de manière indépendante des utilisateurs
 - sans avoir besoin de connaître totalement le parc de machines à protéger

- Réalisable sur une machine, de manière logicielle
 - pour protéger la machine elle-même
 - par l'administrateur de celle-ci

- Le filtrage n'est pas toujours parfait
 - configurations complexes, hétérogènes, etc
 - exploitation parfois délicate
 - tests difficiles à réaliser
 - fonctionnalités ne correspondant pas aux besoins

- Le filtrage n'est pas toujours possible ou facile

Exemple :

- R-commandes
- protocoles basés sur les RPCs : NFS, NIS

La double sécurité

- Les erreurs sont courantes
 - ⇒ La sécurité doit être basée
 - sur le routeur **et**
 - sur la machine
- Probabilité d'erreur simultanément sur les deux très faible

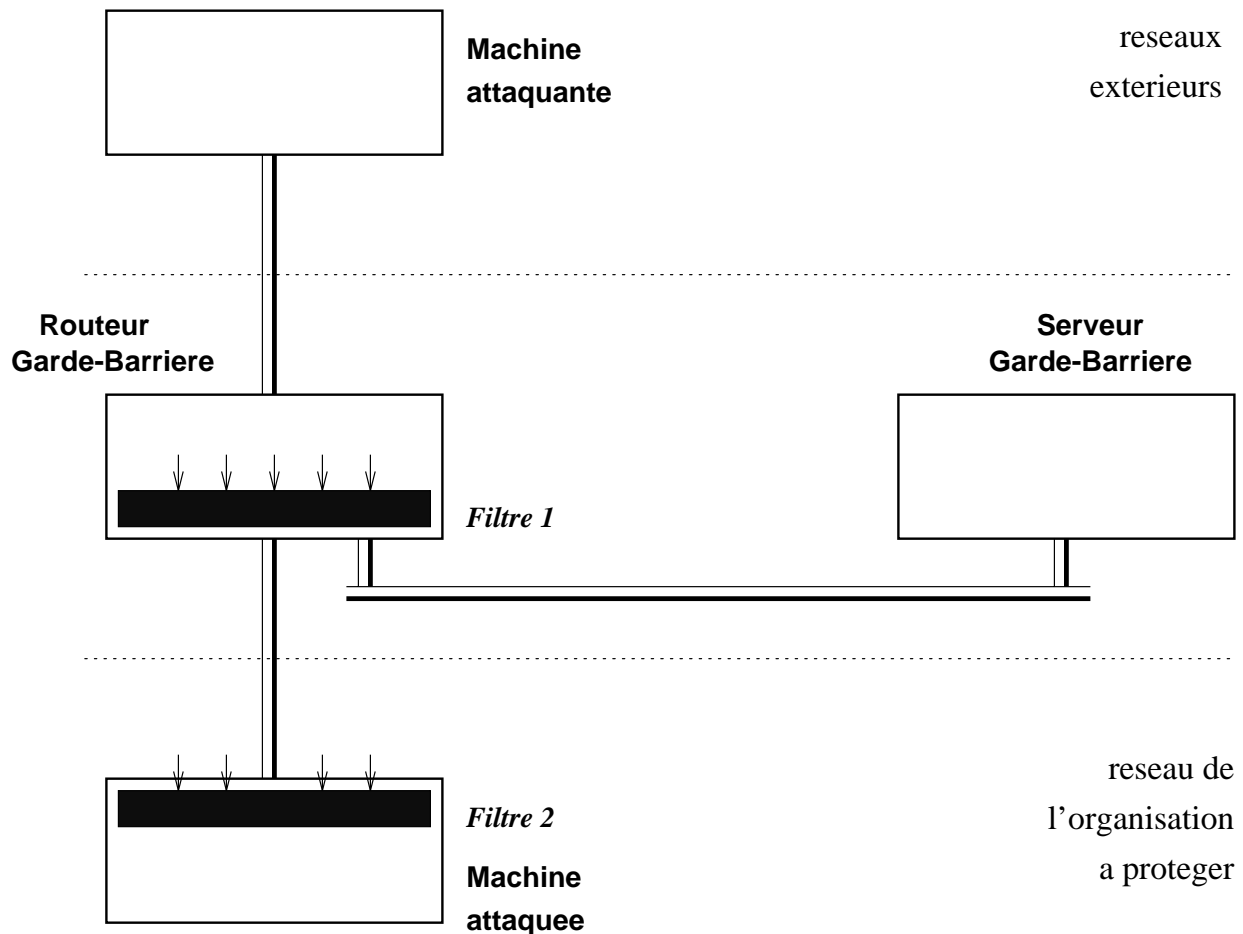


Figure 1. Exemple : Filtrage sur un routeur et sur une machine

La double sécurité

- Possible aussi de sécuriser le Garde-Barrière lui-même avec deux routeurs
- Chaque configuration de l'un est testée en exploitation avant de changer celle de l'autre

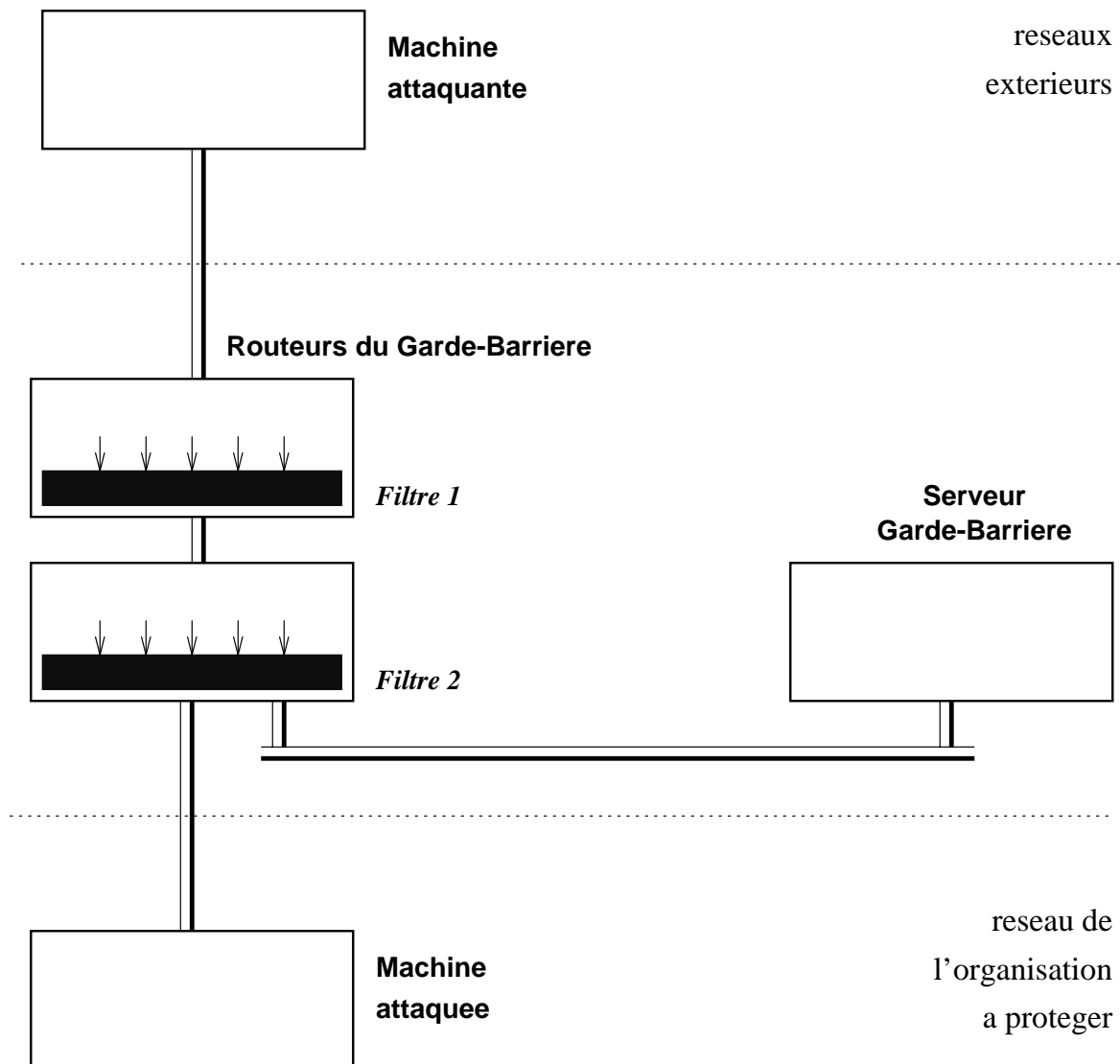


Figure 2. Exemple : Filtrage sur deux routeurs en série

III. Fonctionnement du filtrage IP

III.1 Les critères de filtrage

Chaque communication sur TCP/IP est identifiée par :

((@IP source, n° de port source),
(@IP destination, n° de port destination))

Il sera possible de filtrer à chaque niveau des couches de l'architecture IP, en fonction :

- du port d'entrée ou de sortie physique du routeur,
Exemples : Ethernet, FDDI, synchrone, asynchrone
- des adresses de niveau inférieur à IP,
Exemples : Ethernet, X25
- des adresses IP sources et destination, c'est-à-dire des réseaux et des machines,
- du type de datagramme IP
Exemples : Etablissement de connexion, niveau de confidentialité
- du type de protocole au-dessus de IP,
Exemples : ICMP, TCP, UDP
- des n° de ports sources et destination, c'est-à-dire des services,
Exemples : Telnet, FTP, DNS, SMTP

III.2 Gestion des datagrammes filtrés

Pour chaque datagramme IP, il sera possible :

- de le laisser passer,
 - en le laissant aller vers sa destination
 - en l'envoyant vers une destination qui n'était pas la sienne
- de ne pas le laisser passer, et donc de l'envoyer à la poubelle,
 - sans avertir l'émetteur
 - en avertissant l'émetteur avec un message d'erreur
 - indiquant l'interdiction de passage
 - indiquant "*Host/Network unreachable*"

III.3 Le cas de TELNET

- Le client telnet établi la liaison vers le serveur telnetd qui va contenir la frappe de l'utilisateur.
- Le serveur telnetd établi la liaison vers le client telnet qui va contenir l'écho du serveur.
- Il y a un canal, mais toujours bidirectionnel.

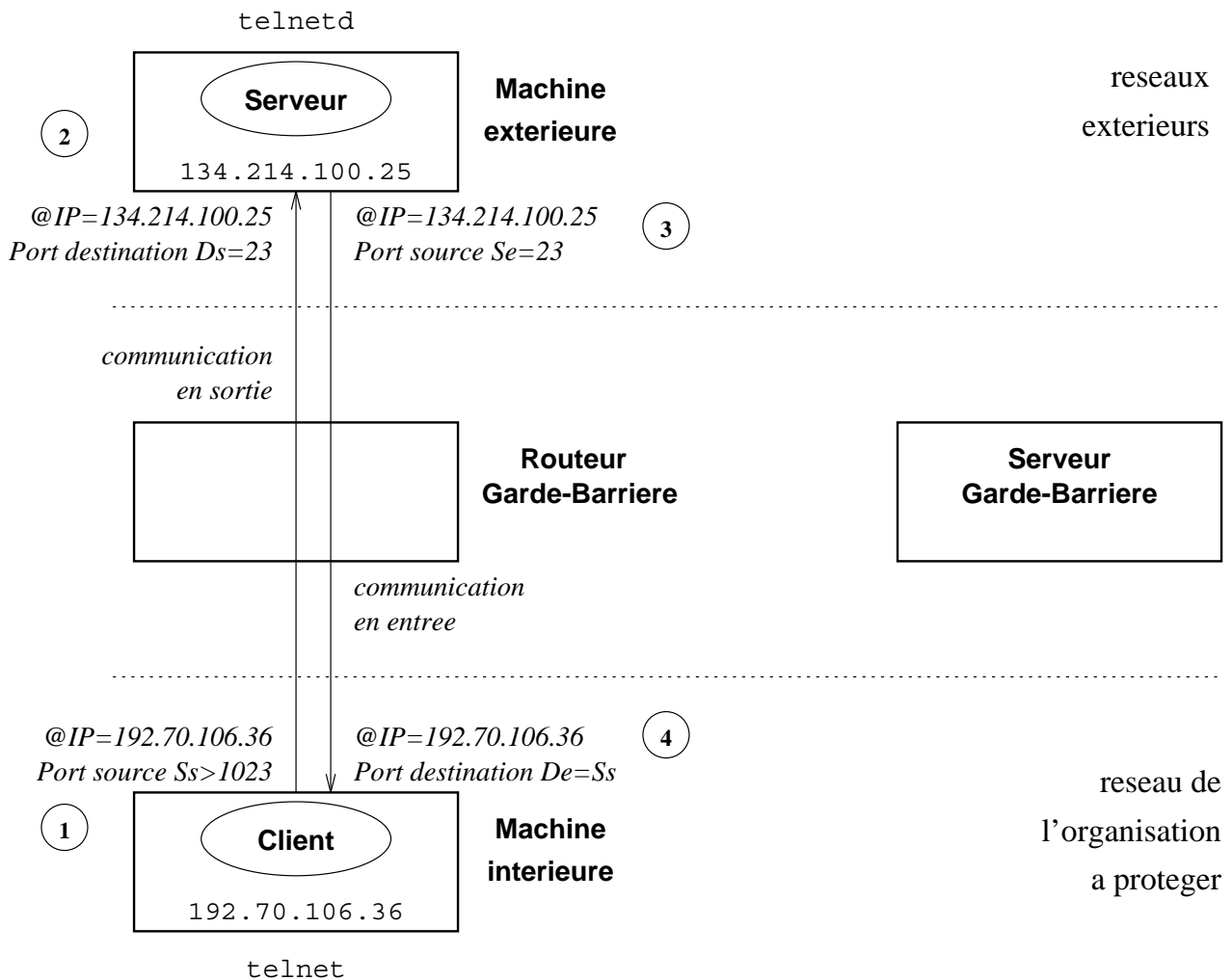


Figure 3. Identification des datagrammes avec une connexion telnet de l'intérieur vers l'extérieur

IV. Les routeurs

- La base de la sécurité

- CISCO
 - Fonctionnalités de filtrage complètes
 - Pas de filtrage en entrée
 - Bonne intégration à la sécurité en utilisant Extended-TACACS
 - Peu d'intérêt pour développer le marché IP

- NSC
 - Fonctionnalités de filtrage complètes
 - Filtres bidirectionnels sur chaque port
 - Permet une construction simple de filtres complexes
 - Le meilleur produit pour un Gare-Barrière

- Wellfleet
 - Seul le haut de gamme est utilisable
 - Fonctionnalités de filtrage minimum

- 3COM
 - Fonctionnalités de filtrage souvent insuffisantes

- Proteon
 - Fonctionnalités de filtrage minimum

- KA9Q, PC-TCP, Netblazer

V. Le relayage

V.1 Le concept du relayage

- Les services de relayages sont des démons tournant sur une machine intermédiaire
- Cette machine est typiquement le serveur du Garde-Barrière.
- Un bon service de relayage n'impose pas de client ou de serveur spécifique.
- Largement intégré sur l'ensemble des connexions Internet sécurisées sur la planète.

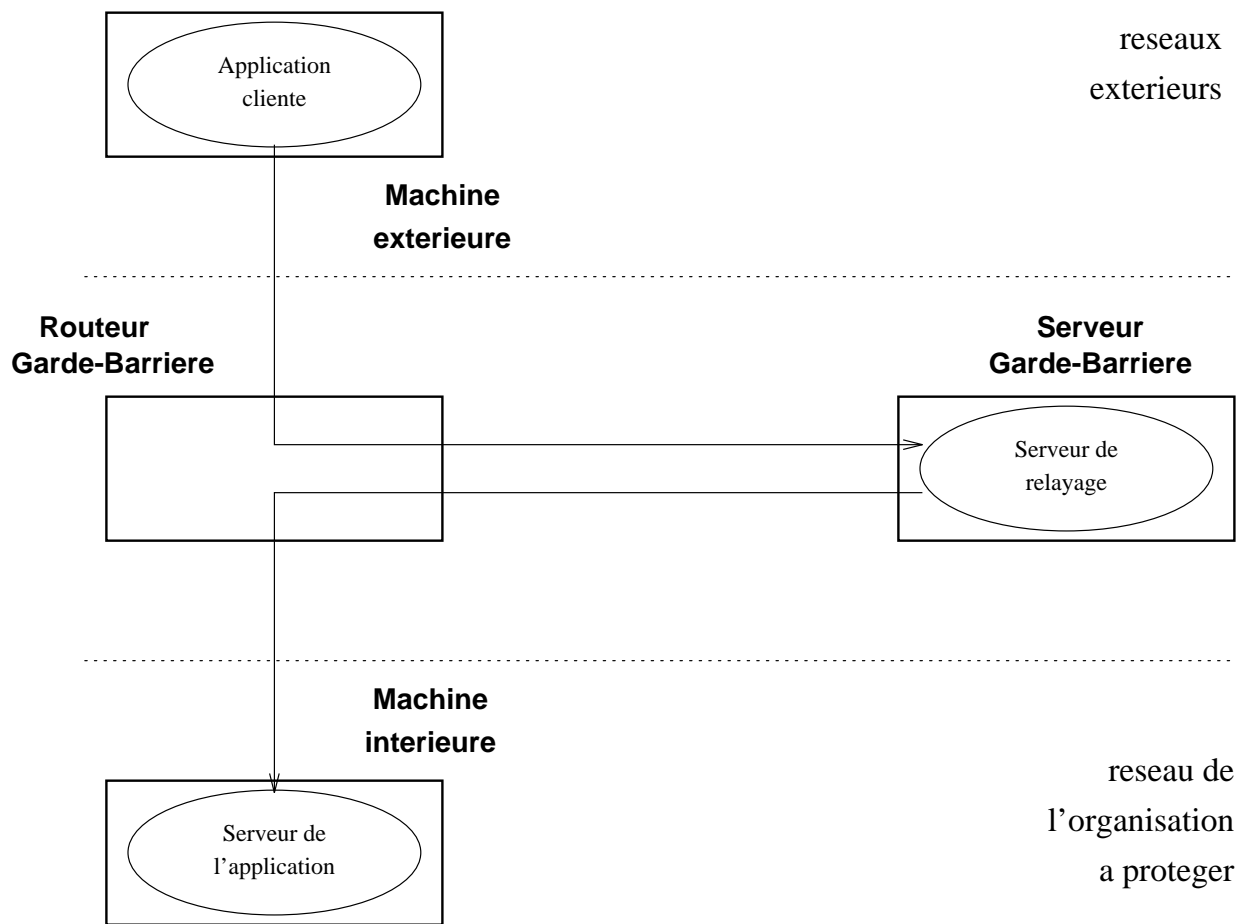


Figure 4. Architecture du relayage

V.2 Le principe du relayage

- Les services de relayages permettent :
 - d'identifier l'utilisateur
 - de l'authentifier
 - de limiter ses autorisations par un filtrage
 - en fonction de l'utilisateur authentifié
 - en fonction de la source et de la destination de celui-ci
 - indépendamment
 - de l'authentification éventuelle sur la machine source
 - de la sécurité distribuée
 - sous un contrôle central, indépendamment de l'administration et de l'exploitation dans l'organisation.

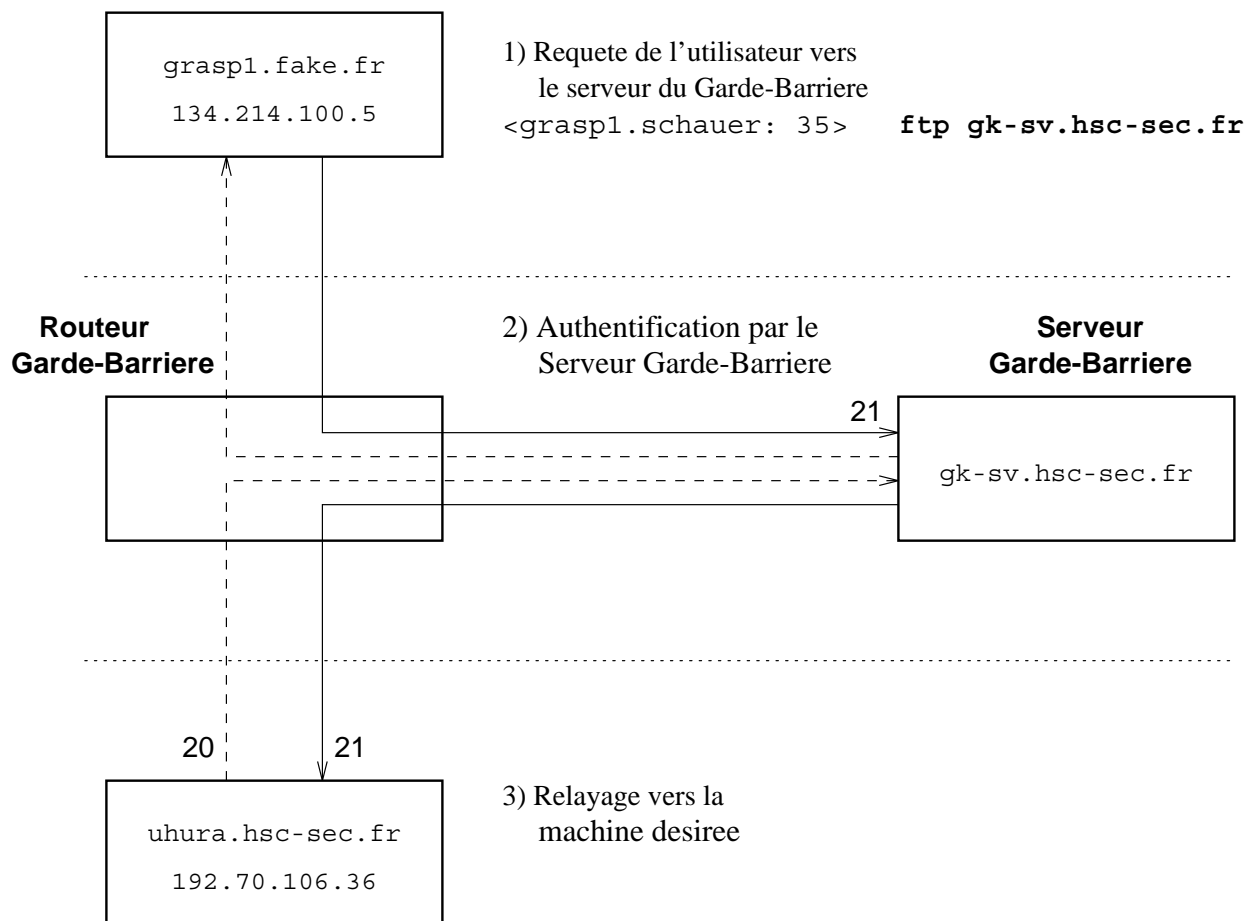


Figure 5. Principe du relaying : *Exemple* avec FTP

Exemple de session pour l'utilisateur :

```
<zephyr.schauer: 1> telnet gatekeeper.hsc-sec.fr
Trying 192.70.106.33 ...
Connected to gatekeeper.hsc-sec.fr.
Escape character is '^['.
```

```
HSCgate login: schauer
Challenge: 36183997
Password: je saisis la réponse renvoyée par ma calculette
Host (or /password or /end): pacte.cnes.fr
```

Access authorized

```
Serveur PACTE login: schauer
Password: je saisis mon mot de passe sur le serveur PACTE
Host (or /password or /end): sisun.cnes.fr
```

```
*****
*                                     *
*               C.N.E.S               *
*                                     *
*               Serveur PACTE         *
*                                     *
*****
```

Access authorized

SunOS UNIX (sisun)

```
*** SYSTEME A ACCES CONTROLE ***
Si apres plusieurs tentatives, vous ne parvenez pas
a vous connecter, contactez votre administrateur au
poste 12345 ou par mail a postmaster@sisun.cnes.fr
```

```
login: schauer
password: je saisis mon mot de passe sur la machine sisun
```

L'exemple ci-dessus a été effectué sur un garde-barrière HSC disposant de l'option d'authentification *Securenet Key*, puis d'un autre utilisant le mot de passe comme authentifieur.

V.3 Les services de relayage

- Solution logicielle, chaque service de relayage (*proxy service*) est généralement un démon.
- Certains services supportent naturellement le relayage.
Exemples : SMTP, NNTP, NTP
- Certains services ont une conception intégrant un relayage.
Exemples : Finger, DNS, whais
- Certains services permettent le développement d'un relai.
Exemples : TELNET, FTP, rlogin
- Certains services peuvent permettre des développements de relais, mais plus difficilement.
Exemples : X11, SQLnet, lpd, Archie, Gopher, WWW
- Certains services ne permettent pas un relayage.
Exemples : NFS, services client/serveur de SGBD, *FrameBuffer* ou applications avec des supercalculateurs ou multimédia, NIS, Licenses flottantes, etc

V.4 Les logiciels de relayage (*proxy services*)

- *Exemple : IGateway* (Internet Gateway) de Sun Consulting
 - Serveurs Telnet et FTP pour une machine pare-feu
 - Services clients spécifiques *itelnet* et *iftp*
 - Facilite le passage par une machine intermédiaire
 - Clients disponibles en source si licence BSD 4.3-Reno
 - Supporte désormais les clients non-Sun
 - Non-disponible hors de l'Amérique du Nord
 - Publicité interdite en France
 - Commercial et prix élevé

-
- *Exemple : HSC-GK* (High Security Concept GateKeeper) de HSC
 - Le plus ancien
 - Serveurs de relayage Telnet, FTP,archie et lpd
 - Utilisation de clients standards
 - Sources des serveurs de relayage fournis
 - Commercial

 - *Exemple : DEC SEAL*
 - Concept identique à HSC-GK
 - Serveurs de relayage X11 avec Xforward
 - Sources des serveurs de relayage fournis
 - Non-disponible hors de l'Amérique du Nord
 - Gratuit et Commercial

- *Exemple* : le TIS Security Toolkit
 - Serveurs de relayage Telnet, FTP, rlogin et service générique
 - Utilisation de clients standards
 - Sources des serveurs fournis
 - Distribué gratuitement

- *Exemple* : *Eagle* de Raptor Systems
 - Revendu sous le nom de *Access IP* par la CSEE
 - Serveurs de relayage Telnet, FTP et service générique
 - Utilisation de clients standards
 - Sources des serveurs de relayages non-diffusés
 - Commercial

- Les outils de développement
 - *Exemple* : la bibliothèque *sockd*
 - Permet de construire son relayage
 - Modification des clients nécessaire
 - Utile pour certains services

VI. Les méthodologies

- Solutions complètes, intégrant toute la méthodologie nécessaire :
- Élément capital de la mise en place d'une sécurité Internet
- *Exemples :*
 - HSC : Garde-Barrière HSC
 - TIS
 - GreatCircle

VII. Les autres produits

VII.0.1 Les pare-feu

- Protection entre un réseau ou un sous-ensemble d'un réseau et l'extérieur,
- Contrôle sur le trafic entre le réseau et l'extérieur,
- Limitation des services possibles à ceux nécessaires.
- Exploitation de la puissance des services sur l'Internet pour les utilisateurs, tout en leur garantissant une sécurité répondant à leur besoin.
- Attention aux risques de services de relayage invisibles !

VII.0.2 Les machines

- En pare-feu avec un produit spécifique :
 - *Exemples de machines* : ATT, DEC, IBM, Sun,
 - *Exemple de logiciels* : HCONS de Sun, *screend*, Netgate de SmallWorks, *log_tcp*, etc

- En complément d'un routeur dans un garde-barrière :
 - Qualité de l'implémentation des services réseaux et de la bibliothèque *sockets*
 - Capacité de charge *syslog()*
 - Capacité de traitement des données
 - Robustesse

VII.0.3 Les boitiers

- Passerelles filtrant les datagramme IP non-authentifiés
- *Exemple* : Passerelle SIS de Ace Timing
- Coupure entre réseaux TCP/IP
- Authentification externe sur les postes extérieurs au réseau
- Contrôle de l'authentification dans chaque datagramme

VII.0.4 Les cartes et calculettes

- Permettent d'authentifier les utilisateurs, sans utiliser un mot de passe transitant en clair sur les réseaux.
- Cartes à puces
Exemples : GemPlus, Ace Timing
- Calculettes basées sur le temps
Exemple : SecureID de Security Dynamics
- Calculettes basées sur un DES initialisé dans la calculette
Exemple : SecureNetKey de Digital Pathways
- Calculettes DES à lecture optique
Exemples : ADV Technologies, Cyclop
- Existe d'autres méthodes comme le mot de passe unique : SKey

VIII. Le rôle des CERTs

- Centralisent les incidents de sécurité,
- Organisation hiérarchique,
- Le CERT général est à l'université Carnegie-Mellon (*cert.org*),
- Il faut avoir un CERT local au service sécurité informatique,
- Lui seul pourra contacter le CERT de niveau supérieur si cela est nécessaire,
- Un CERT au niveau national, ou au niveau du réseau à l'échelle nationale, est souvent souhaitable.

IX. Mise en place d'une passerelle

- Procédure longue et couteuse;
- Ne peut pas se décider à la légère;
- Devient indispensable, avec l'importance des réseaux et l'importance de la sécurité;
- Doit être intégré aux mentalités \Rightarrow plus on attends, plus la mise en oeuvre est couteuse;
- Demande généralement l'existence d'un service sécurité indépendant des services gérant des pare-feu, pour vérifier, valider et agréer les pare-feu, comme les machines ayant des accès sur l'extérieur;
- Nécessite des administrateurs disponibles et compétants pour gérer le pare-feu ou le garde-barrière.

Sommaire

I. Modèles possibles de passerelles TCP/IP	4
II. Le filtrage IP	5
III. Fonctionnement du filtrage IP	9
III.1 Les critères de filtrage	9
III.2 Gestion des datagrammes filtrés	10
III.3 Le cas de TELNET	11
IV. Les routeurs	12
V. Le relayage	14
V.1 Le concept du relayage	14
V.2 Le principe du relayage	16
V.3 Les services de relayage	19
V.4 Les logiciels de relayage (<i>proxy services</i>)	20
VI. Les méthodologies	24
VII. Les autres produits	25
VII.0.1 Les pare-feu	25
VII.0.2 Les machines	26
VII.0.3 Les boitiers	27
VII.0.4 Les cartes et calculettes	28

VIII. Le rôle des CERTs	29
IX. Mise en place d'une passerelle	30

LIST OF FIGURES

Figure 1. <i>Exemple</i> : Filtrage sur un routeur et sur une machine	8
Figure 2. <i>Exemple</i> : Filtrage sur deux routeurs en série	9
Figure 3. Identification des datagrammes avec une connexion telnet de l'intérieur vers l'extérieur	12
Figure 4. Architecture du relayage	15
Figure 5. Principe du relayage : <i>Exemple</i> avec FTP	17