

Réseaux informatiques

RXI

Chapitre 8

Firewall

Objectifs d'apprentissage

- Savoir expliquer les principaux objectifs de la sécurité réseau
- Savoir expliquer les fonctions d'un firewall et ses limites
- Savoir expliquer les fonctions des types d'équipements: filtre de paquets, passerelle applicative, serveur bastion
- Savoir expliquer les principales architectures de firewalls et leurs caractéristiques



Sécurité des réseaux

- Que faut-il protéger ?

Les données – les ressources – la réputation

Objectifs de sécurité (CIA)

Confidentialité des données

- Protection des données d'une divulgation non autorisée

Intégrité des données

- Empêcher une modification non autorisée

Disponibilité des données

- Garantir l'accès légitime aux données

Authentification de l'origine

- Être sûr de l'identité de la source des données

Disponibilité des ressources

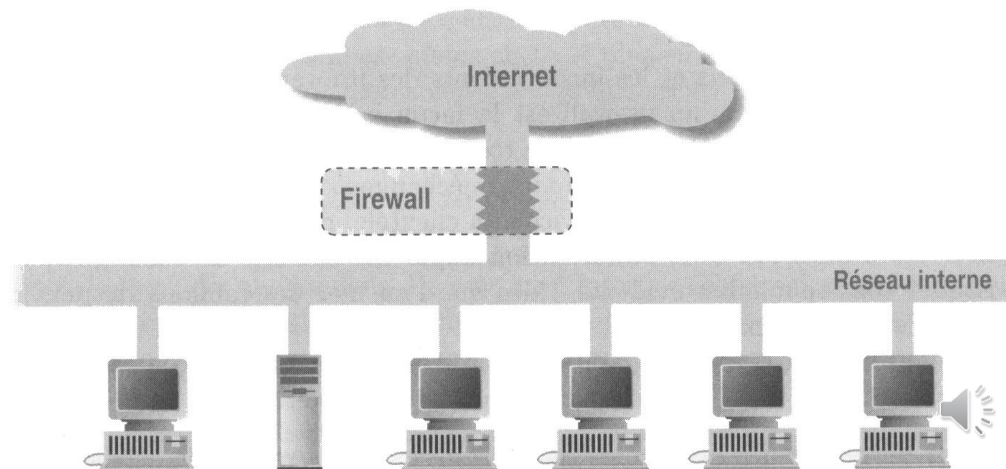
- Protéger les ordinateurs/réseaux d'une utilisation illégitime



Le firewall (pare-feu)

Un firewall empêche les dangers provenant de l'extérieur de se répandre à l'intérieur du réseau

- Il restreint l'accès à un point précis
- Il empêche les agresseurs de s'approcher de vos autres défenses
- Il restreint la sortie à un point précis



Fonctions d'un firewall

Centre de décision de sécurité

- Goulet d'étranglement par où passe tout le trafic

Impose le règlement de sécurité

- Sert à implémenter la politique de sécurité
(p.ex. la restriction d'accès aux services dangereux sur Internet)

Monitor du trafic depuis l'extérieur

- Permet de collecter des informations sur l'utilisation de services

Limite l'exposition du réseau

- Un firewall interne peut confiner un problème de sécurité dans une partie du réseau



Un firewall ne protège PAS...

... contre des utilisateurs internes malveillants

- Si un attaquant se trouve déjà à l'intérieur du réseau, un firewall n'offre pas de protection

... contre des connexions qui ne passent pas par lui

- Par exemple, un point d'accès WLAN mal sécurisé peut permettre à un attaquant d'accéder le réseau sans passer par le firewall

... contre des virus / vers

- Un firewall (réseau) n'examine pas les données du niveau application
- Il faut un autre dispositif: une ALG (*Application Layer Gateway*) ou un IDS (*Intrusion Detection System*)



Stratégies de sécurité

Refus par défaut

« Ce qui n'est pas expressément autorisé est interdit »

- Choix évident du point de vue de l'administrateur
- Difficile à comprendre pour les utilisateurs

Permission par défaut

« Ce qui n'est pas expressément interdit est autorisé »

- Suppose que les utilisateurs connaissent les dangers
- **Vouée à l'échec**
 - Course contre les nouveaux services, les nouvelles failles, les nouvelles idées des utilisateurs

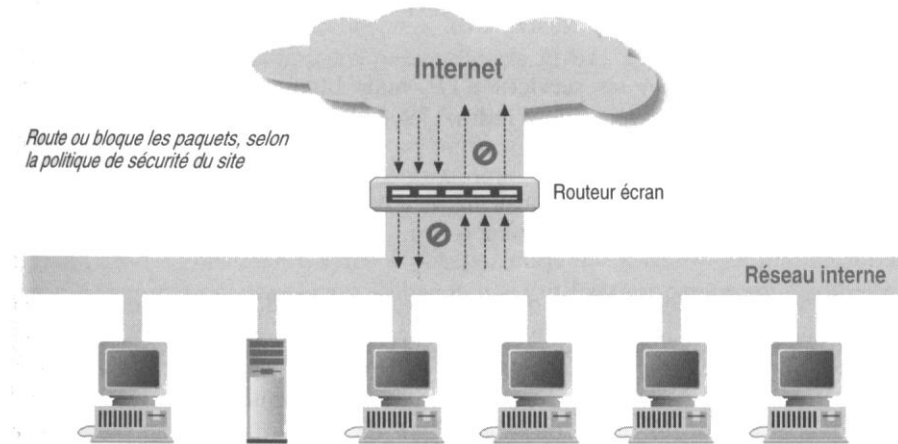


Types d'équipements

1) Filtre de paquets

« Routeur écran » ou « firewall réseau »

- Achemine de manière sélective les paquets entre Internet et le réseau interne
- Filtre les paquets entrants et sortants selon :
 - Les **informations des en-têtes IP et TCP** (IP source et destination, port source et destination, protocole, ...)
 - Les **informations de routage** (interface d'entrée, interface de sortie)



Source: Chapman/Zwicky



Exemple de configuration du filtrage

- Sur Linux, avec la commande iptables
 - Configuration de la machine comme firewall (chaîne FORWARD)
- Refus par défaut

```
> iptables -F           # Flush: effacer toutes les règles
> iptables -P INPUT DROP # Chaîne INPUT -> destiné à la machine
> iptables -P OUTPUT DROP # Chaîne OUTPUT -> généré par la machine
> iptables -P FORWARD DROP # Chaîne FORWARD -> traverse la machine
```

- Ouvrir l'accès SSH au serveur 10.1.1.1

```
> iptables -t filter -A FORWARD -d 10.1.1.1 -p tcp -dport 22 -j ACCEPT
> iptables -t filter -A FORWARD -s 10.1.1.1 -p tcp -sport 22 -j ACCEPT
```

IP source

IP destination

Port source

Port destination

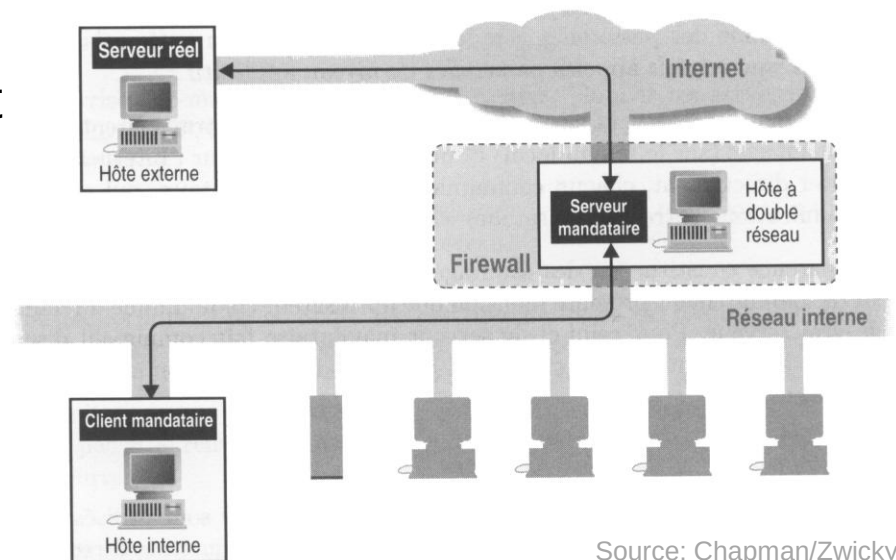


Types d'équipements

2) Passerelle applicative

« Server mandataire » ou « proxy »

- Accepte les requêtes des clients et les redirige vers le vrai serveur
- Respecte la politique de sécurité de l'entreprise
- Transparent pour les utilisateurs
- Doit être complété par un mécanisme qui restreint les communications directes



Source: Chapman/Zwicky

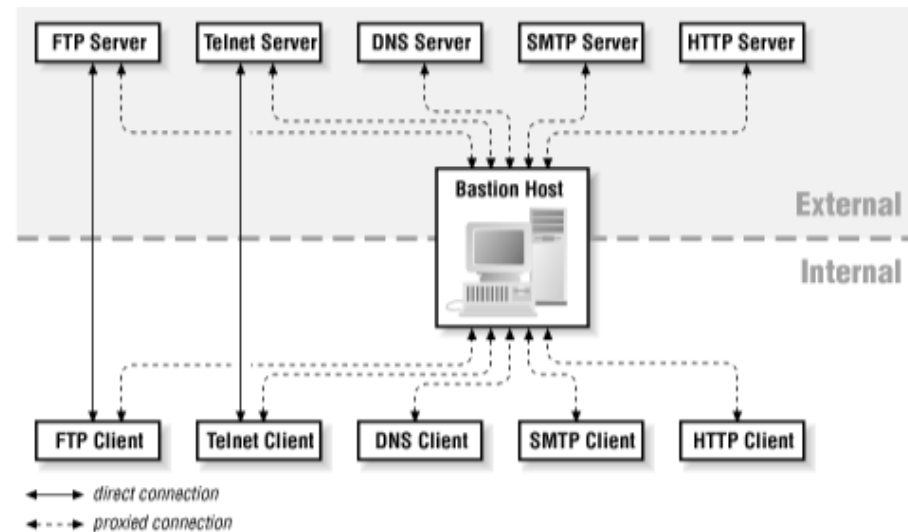


Types d'équipements

3) Machine bastion

Un bastion est un serveur accessible depuis l'extérieur

- Exemples:
serveur Web, serveur email
- Un bastion tout seul réalise un service, mais n'apporte pas de sécurité
- Un serveur bastion doit être sécurisé par d'autres mécanismes



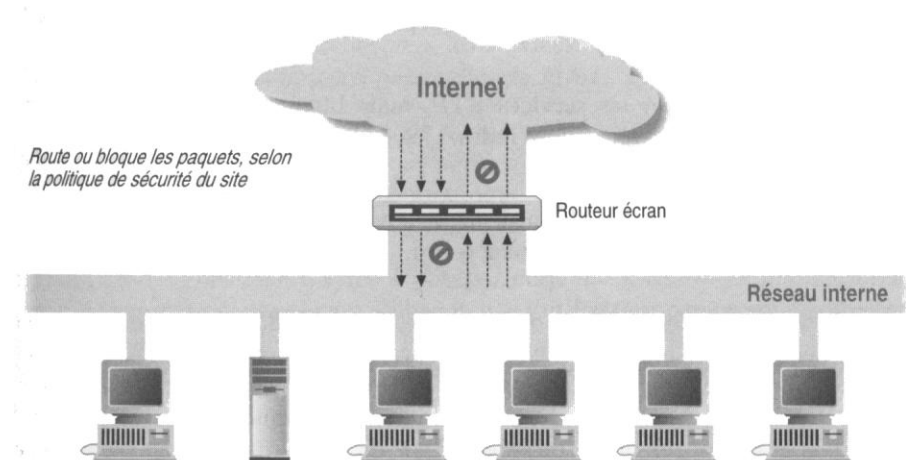
Architecture des firewalls

- Un firewall comprend généralement plusieurs éléments
 - Un ou plusieurs **filtres de paquets**
 - Un ou plusieurs **passerelles applicatives**
 - Un ou plusieurs **réseaux isolés**
- ✓ La sécurité ne dépend pas d'un seul élément
- ✓ L'agresseur doit franchir plusieurs barrières



Architecture : routeur écran simple

- Architecture simple avec un seul niveau de protection
- Utilisé par exemple dans les réseaux à domicile
- Simple à mettre en place
- Niveau de sécurité basic
- Pas de défense en profondeur (une seule barrière à franchir)
- Pas de sécurité applicative

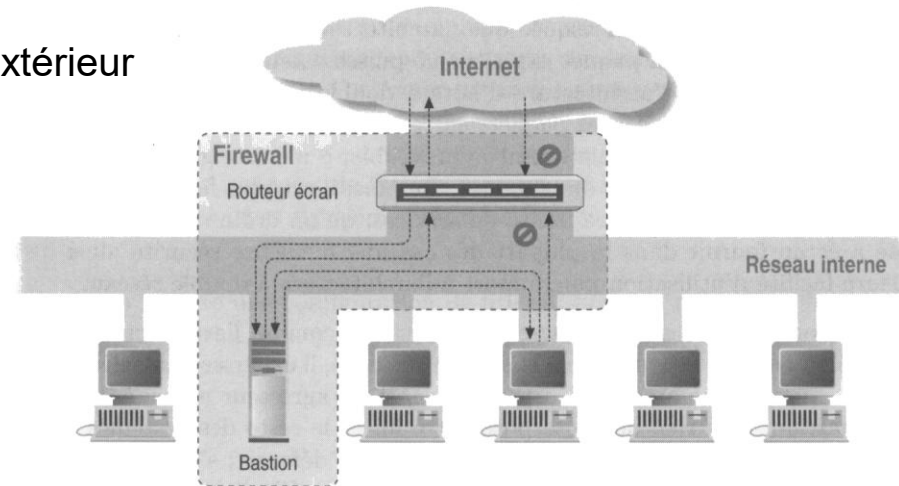


Source: Chapman/Zwicky



Architecture : routeur écran avec bastion

- Machine bastion située sur le réseau interne
 - Bastion est exposé à Internet
 - Bastion peut être un **proxy** pour les connexions depuis l'intérieur ou un **serveur** pour les connexions depuis l'extérieur
 - Peut recevoir des connexions depuis l'extérieur
 - Le routeur écran ne permet que les connexions depuis / vers le bastion



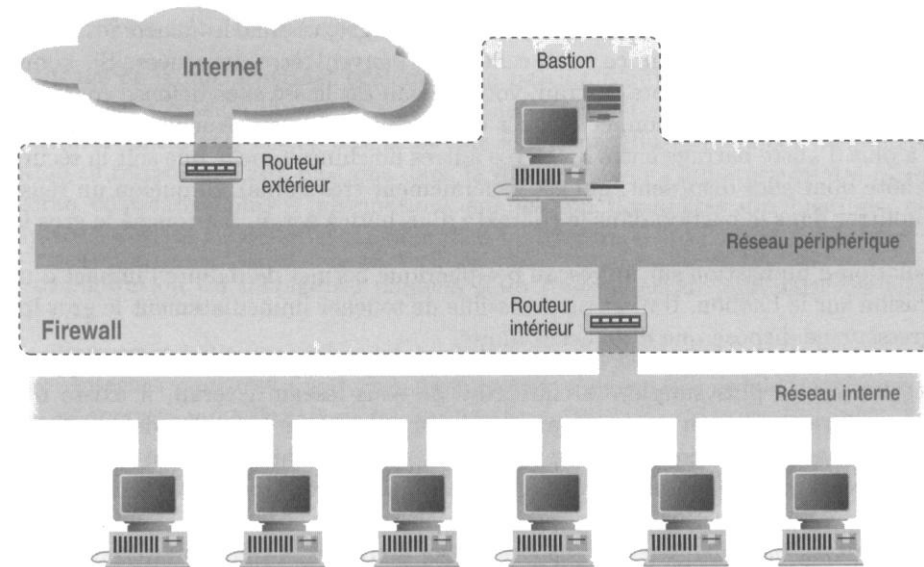
Source: Chapman/Zwicky

- Bon niveau de sécurité (réseau et applicative)
- Le bastion se trouve sur le réseau interne
- Le routeur écran est l'unique point de défense



Architecture : sous-réseau à écran (DMZ)

- Couche de sécurité supplémentaire:
réseau périphérique ou DMZ
(*demilitarized zone*)
 - Isole le bastion, qui est vulnérable aux attaques
 - Un intrus ayant réussi à s'infiltrer sur le bastion doit encore franchir le routeur écran intérieur
 - Le trafic LAN ne peut pas être espionné depuis le bastion
- Solution bien sécurisée
- Solution standard dans les réseaux d'entreprise
- Solution coûteuse

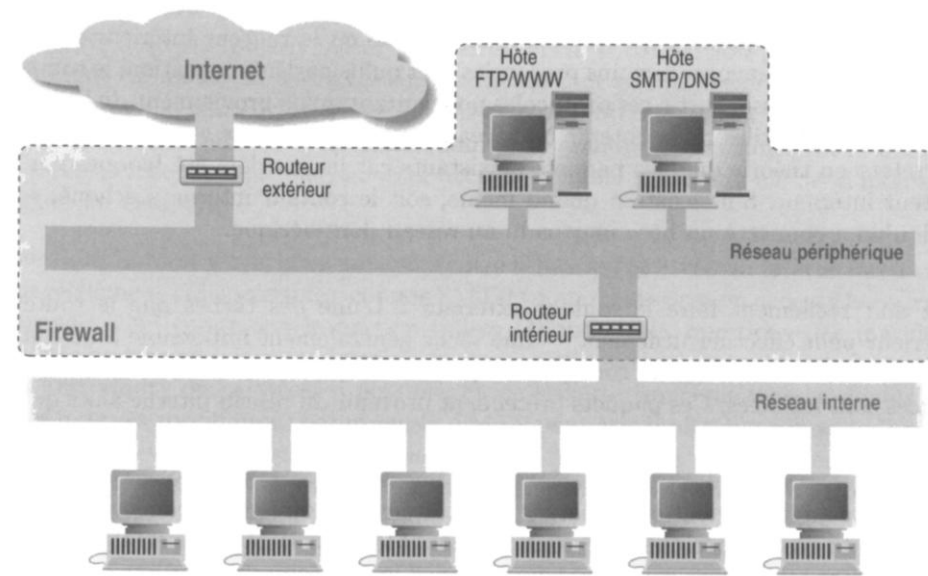


Source: Chapman/Zwicky



Variante : plusieurs bastions

- Séparation des bastions, par exemple
 - Bastions pour les utilisateurs internes (proxy, e-mail) plus serveurs accessibles depuis Internet
- Isolation des services vulnérables (FTP) sur une machine séparée
- Performances améliorées
- Différents niveaux de sécurité
- Solution coûteuse



Source: Chapman/Zwicky

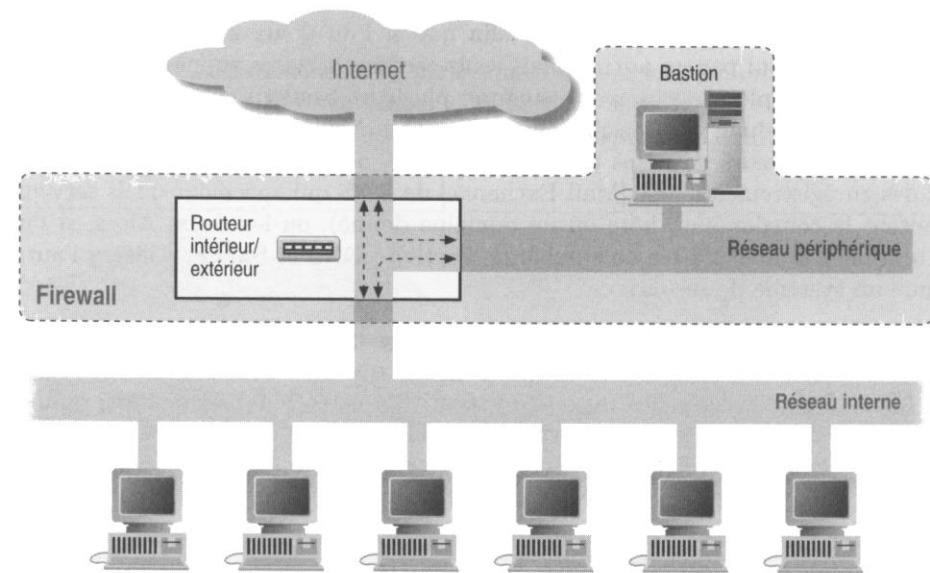


Variante : fusionner routeurs externe et interne

- Le bastion reste isolé sur le réseau périphérique
 - Gère les services critiques
- Le routeur peut autoriser le passage direct de certains services

↑ Ne diminue que peu la sécurité

- Le routeur est le seul élément de défense



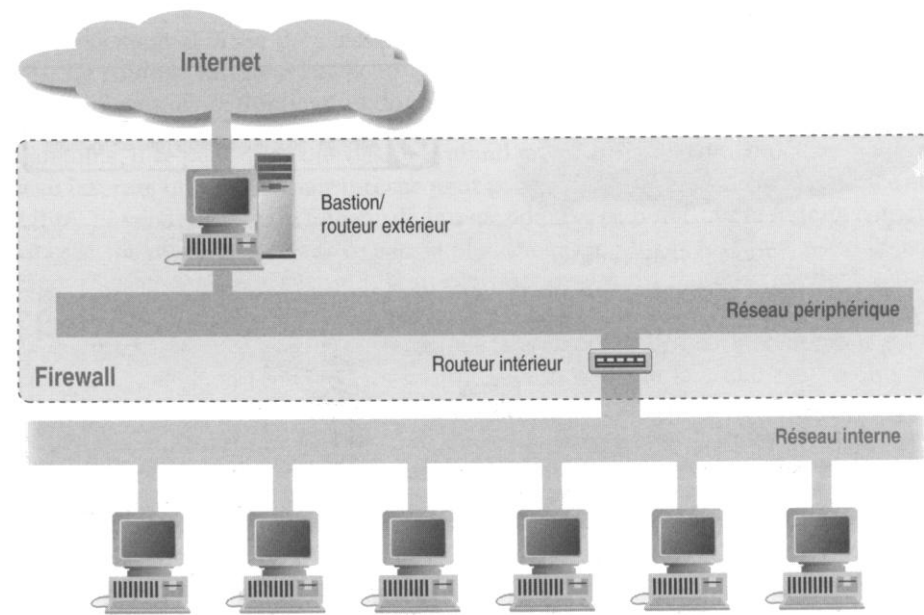
Source: Chapman/Zwicky



Variante : fusionner routeur externe et bastion

- Architecture pratique pour les petits sites
 - Connexion FAI
 - Machine à l'entrée fonctionne comme routeur écran et bastion à la fois

↑ Ne diminue que peu la sécurité



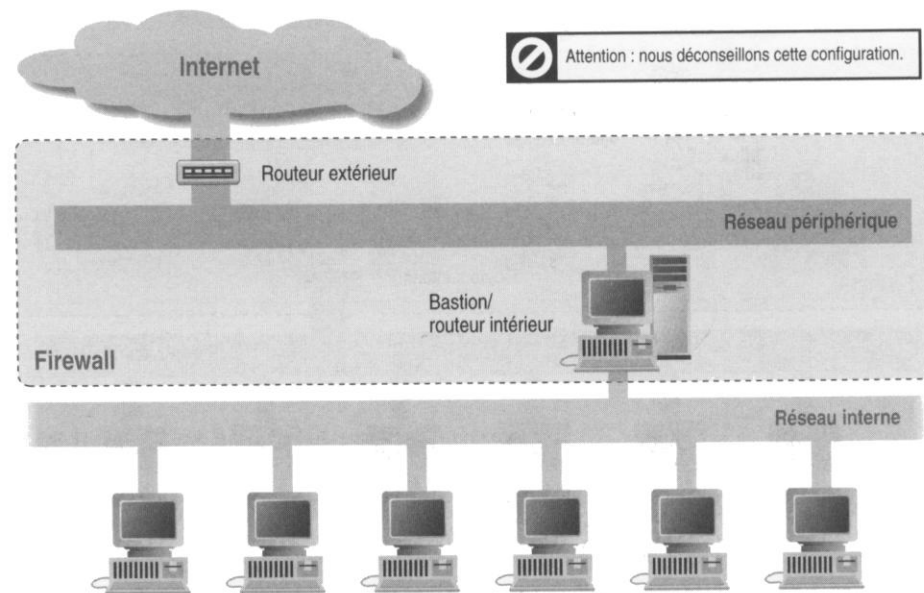
Source: Chapman/Zwicky



Attention :

NE PAS fusionner bastion et routeur interne

- Rend inutile le réseau périphérique
 - Si le bastion est infiltré, l'agresseur a accès au trafic LAN



Source: Chapman/Zwicky



Fin du chapitre