Composants fondamentaux d'une architecture sécurisée

Firewalls

Carlos Aguilar

carlos.aguilar@enseeiht.fr

IRIT-IRT

Plan

Commutation et VLANs

Concentrateur (hub) vs Commutateur (switch)

Hub : chaque paquet reçu dans un port est diffusé dans tous les autres
Switch : ce n'est vrai que quand il ne connaît pas le MAC destination
... ou quand il n'arrive plus à marcher correctement ...

⇒ Utiliser des switchs
⇒ Utiliser la fonction port security
⇒ Sécuriser les locaux des équipements réseau

VLANs

Isolation au niveau 2 (comme s'il y avait plusieurs réseaux locaux physiquement séparés) par plages de ports/MACs/IPs

PVLANs

Par définition : VLAN de taille 1 défini au niveau 1 (notion d'isolated ports)
Exemple : hotel, aeroport, etc. (pas de comm. niveau 2 entre les utilisateurs)

Firewalls : principe

Tout ou rien

Le VLAN défini par plages IP :

- Même VLAN : on communique au niveau 2
- VLAN différent : on envoie au routeur qui décide de faire le pont ou pas

Principe du Firewall

Connecter deux réseaux au niveau 3 avec une politique plus fine que du tout ou rien
Filtrer en fonction :

- du protocole (TCP/UDP/ICMP)
- des ports et IPs origine et destination
- du sens de la connexion

Généralement on sépare la politique entrante et sortante

Firewalls : variantes

Firewalls de type routeur

Firewall sans états (stateless) :

- Examine chaque paquet indépendamment
- Peut bloquer les paquets avec le flag SYN ...

Firewall à etats (statefull) :

- Peut prendre en compte les paquets envoyés dans le passé
- Gestion de Notion de “transmission” UDP (indisp. pour le DNS)
- ICMP, fragmentation, port knocking ...

Firewall Applicatif :

- Protocoles dont les ports sont pas facilement prévisibles
- Vérification du protocole (pour éviter le contournement)

Firewall Personnel

Généralement statefull. ACL en fonction des applications !

Firewalls : problèmes

Authentification basée sur l'IP

Les règles sont définies pour des machines
Contrôle de quelle machine par IP
Lien implicite machine-utilisateur

Tunnels et encapsulation

Tunnels SSH
HTTP CONNECT

Pas de défense en profondeur

Problème principal : les paquets sont routés !
$\rightarrow$ simplification des attaques si une faille est trouvée

Utilisation de relais applicatifs

Intérêt

Authentification des utilisateurs

- Peut utiliser une authentification forte (contrairement à l'IP)
- Mise en place de logs et politique en fonction de l'utilisateur

Mise en place d'une politique de sécurité par protocole

- Scan viral pour SMTP
- Pas de CONNECT en HTTP

Paquets traités : il n'y a que les informations contenues qui passent !

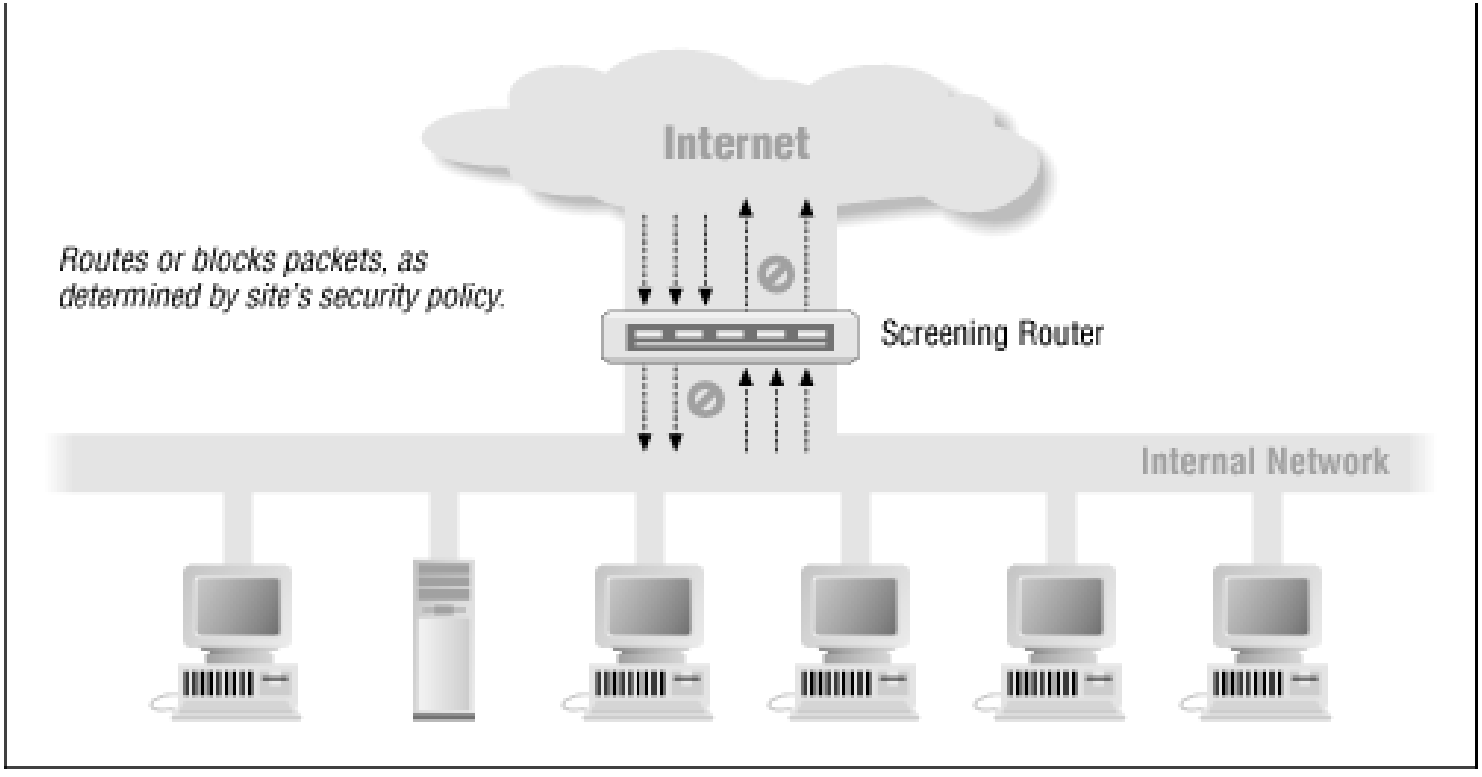
Danger

Plus un programme analyse des données et est complexe plus il est facile de l'attaquer

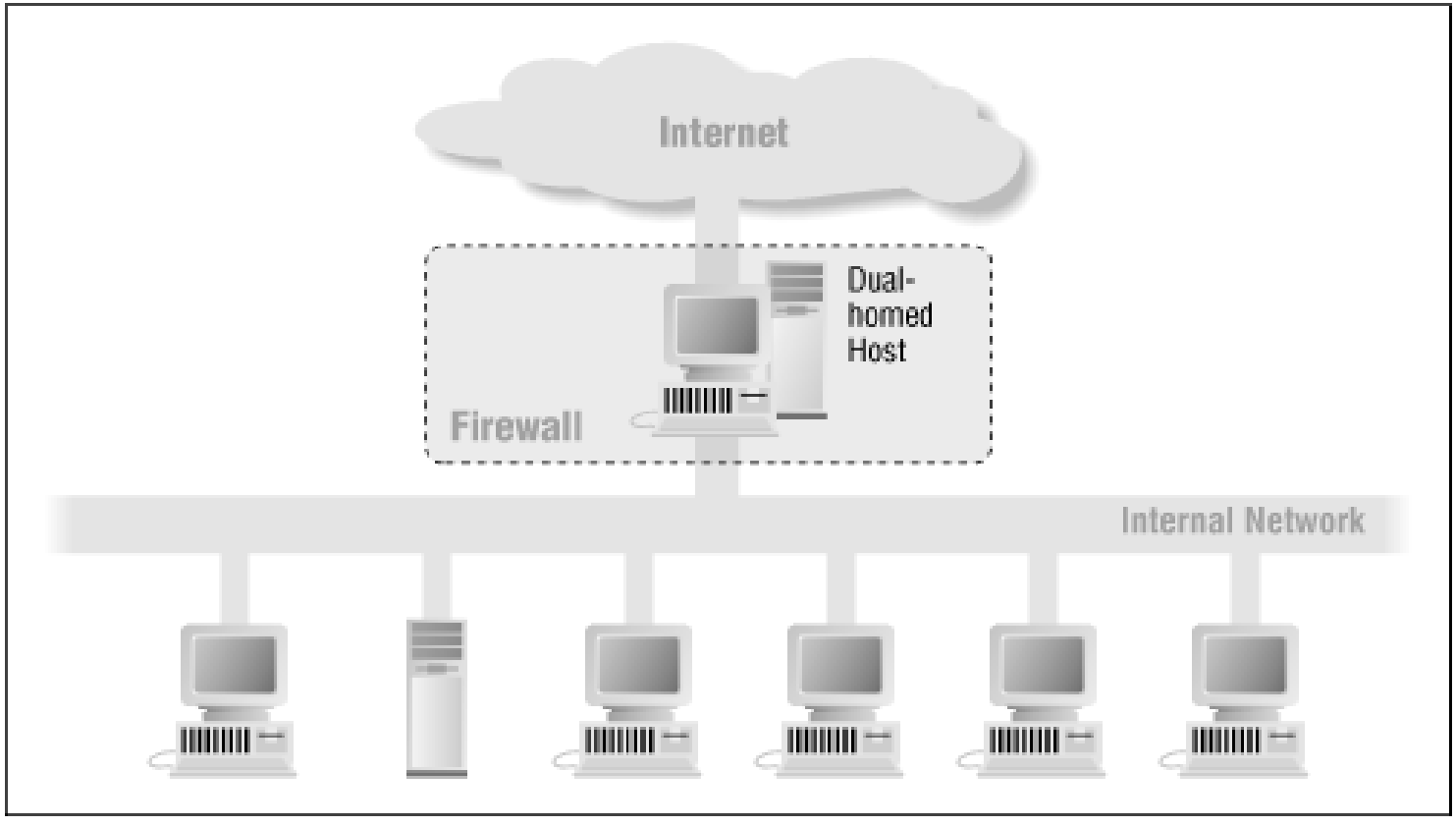
- Réduire les services au minimum
- Audit du bastion/relais
- Prendre en compte qu'il peut être compromis

Plan

Firewalls : architecture de type *screening router*



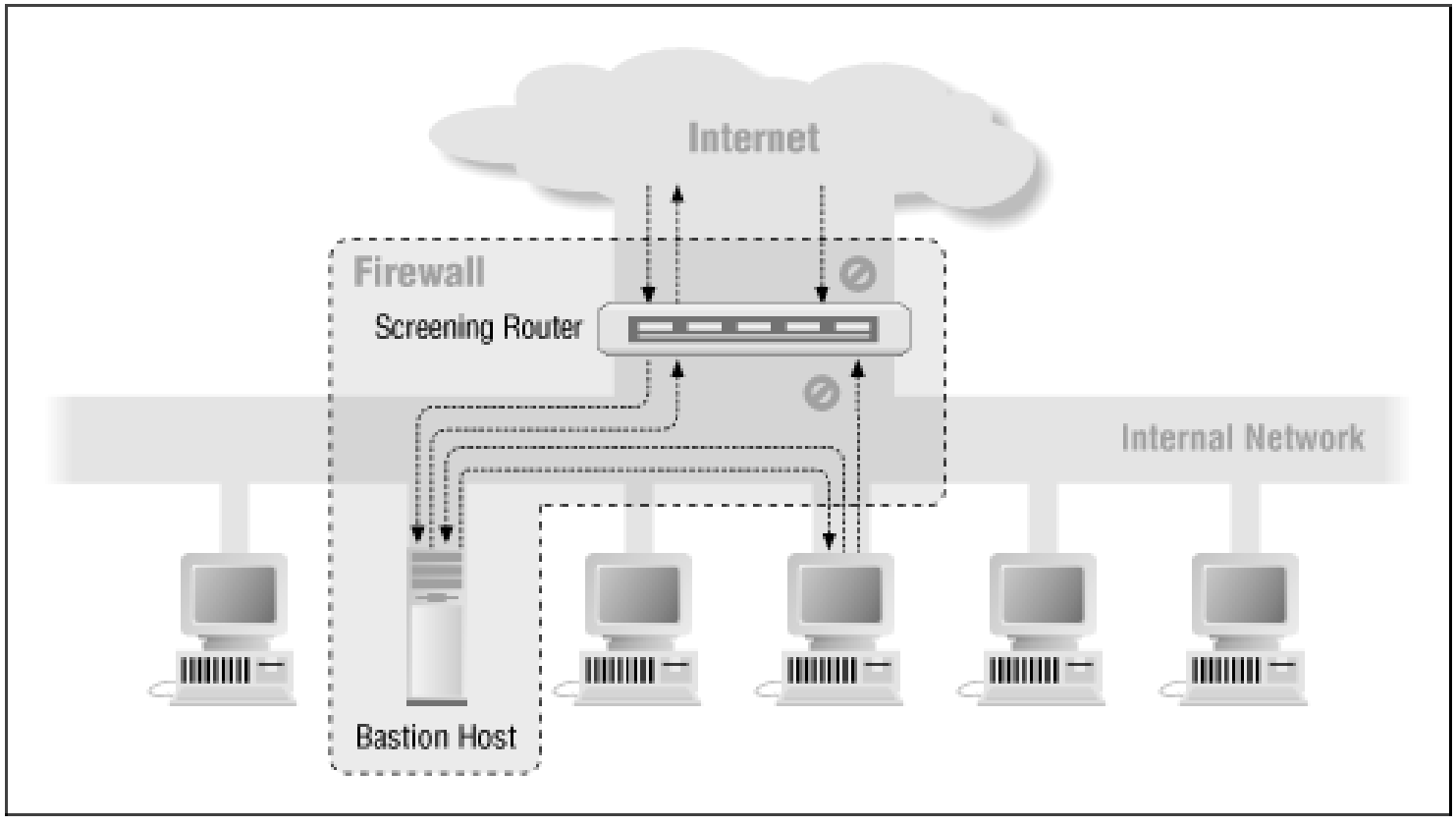
Architecture de type bastion relais



Le bastion ne route pas les paquets !

Mise en place de proxys entrants/sortants pour chaque service

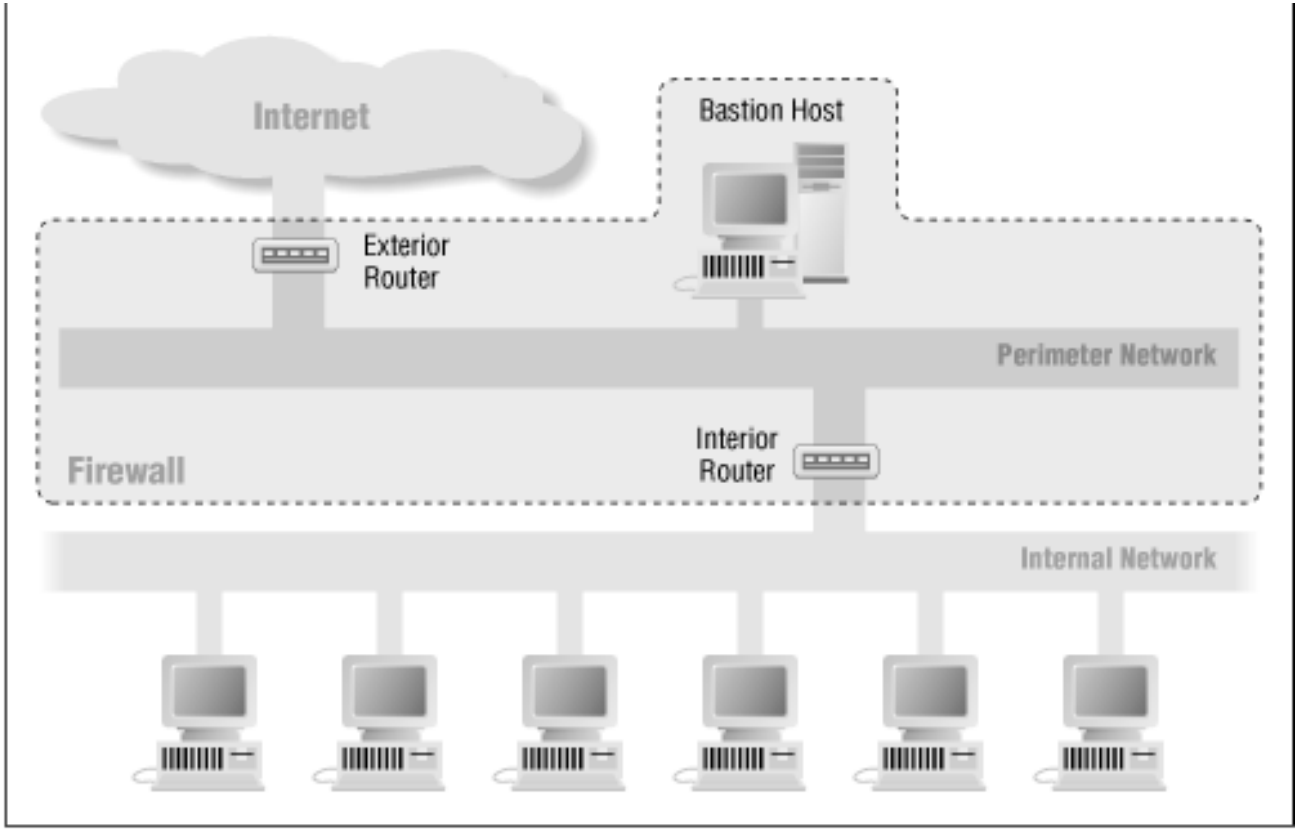
Architecture de type screening router + bastion



Avantages

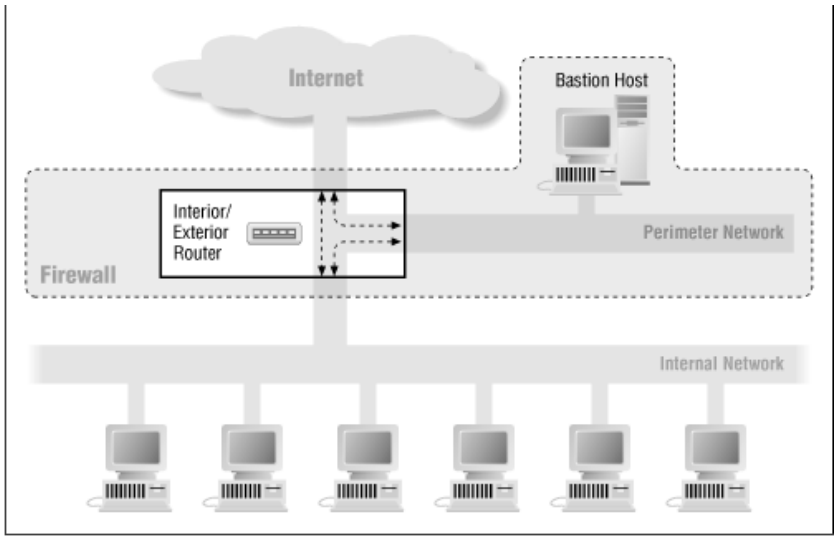
Protège le bastion
Plus modulable (en particulier pour les flux sortants)

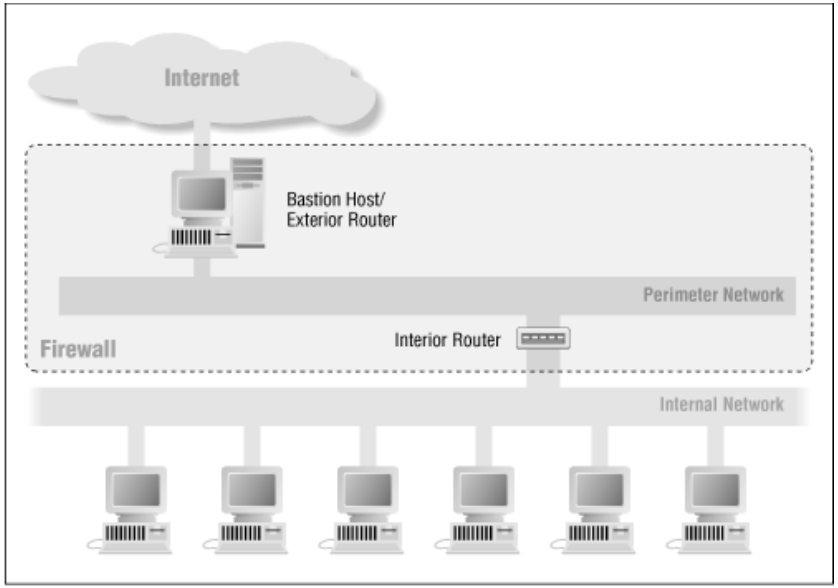
Architecture de type DMZ



Si le bastion tombe $\rightarrow$ architecture de type screening router
Plusieurs serveurs peuvent exister dans la DMZ (serveur web, SMTP, etc.)
Deuxième niveau de DMZ contenant des service (e.g. serveur SQL)

Architecture de type DMZ (variantes)





Moins de boulot

Si le bastion tombe $\rightarrow$ architecture de type screening router ...

Pas vrai si on fusionne le bastion et le routeur interne !

Fin !

Des questions ?