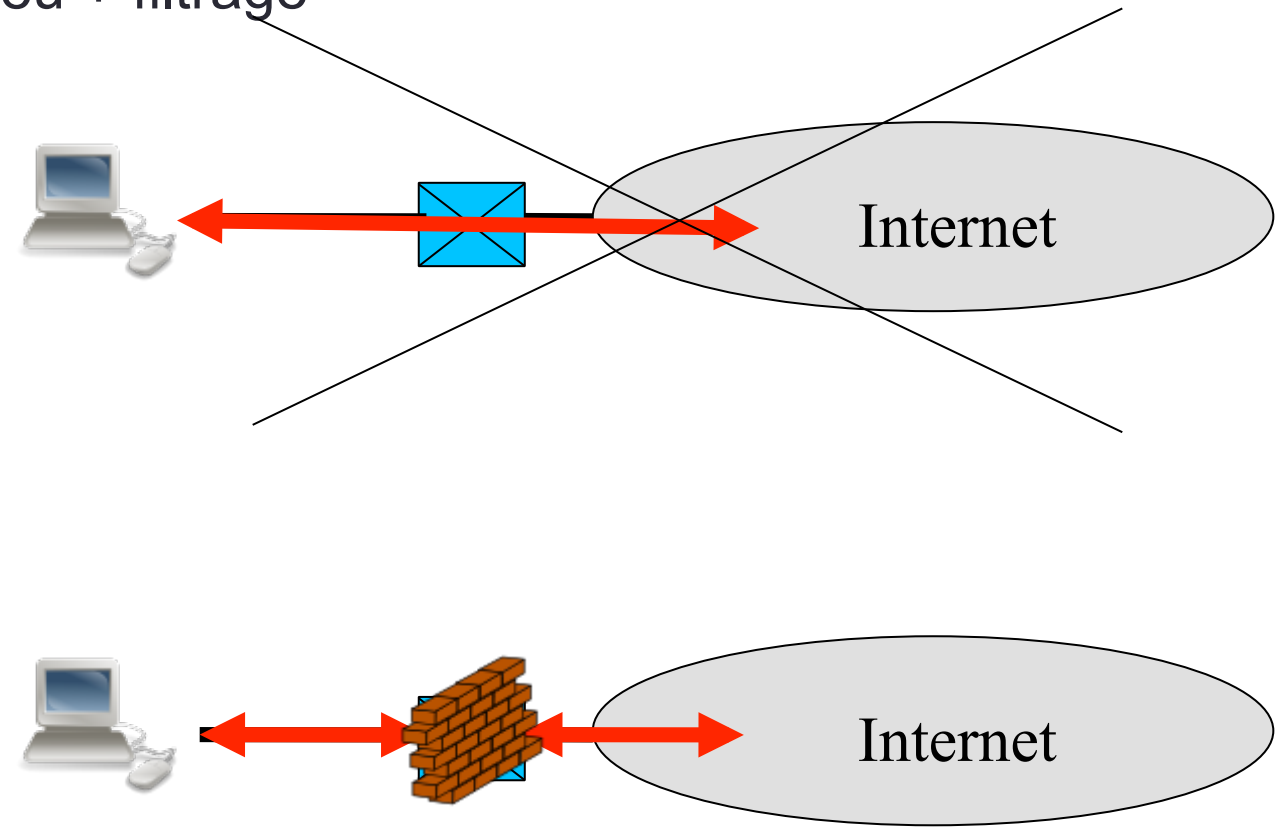
RÉSEAU II : SECURITÉ, FIREWALL, BASTION…

Sources:
lasecwww.epfl.ch
www.cert.org
www.goCSI.com
securit.free.fr
www.cru.fr
www.ssi.gouv.fr

MESURE DE SÉCURITÉ

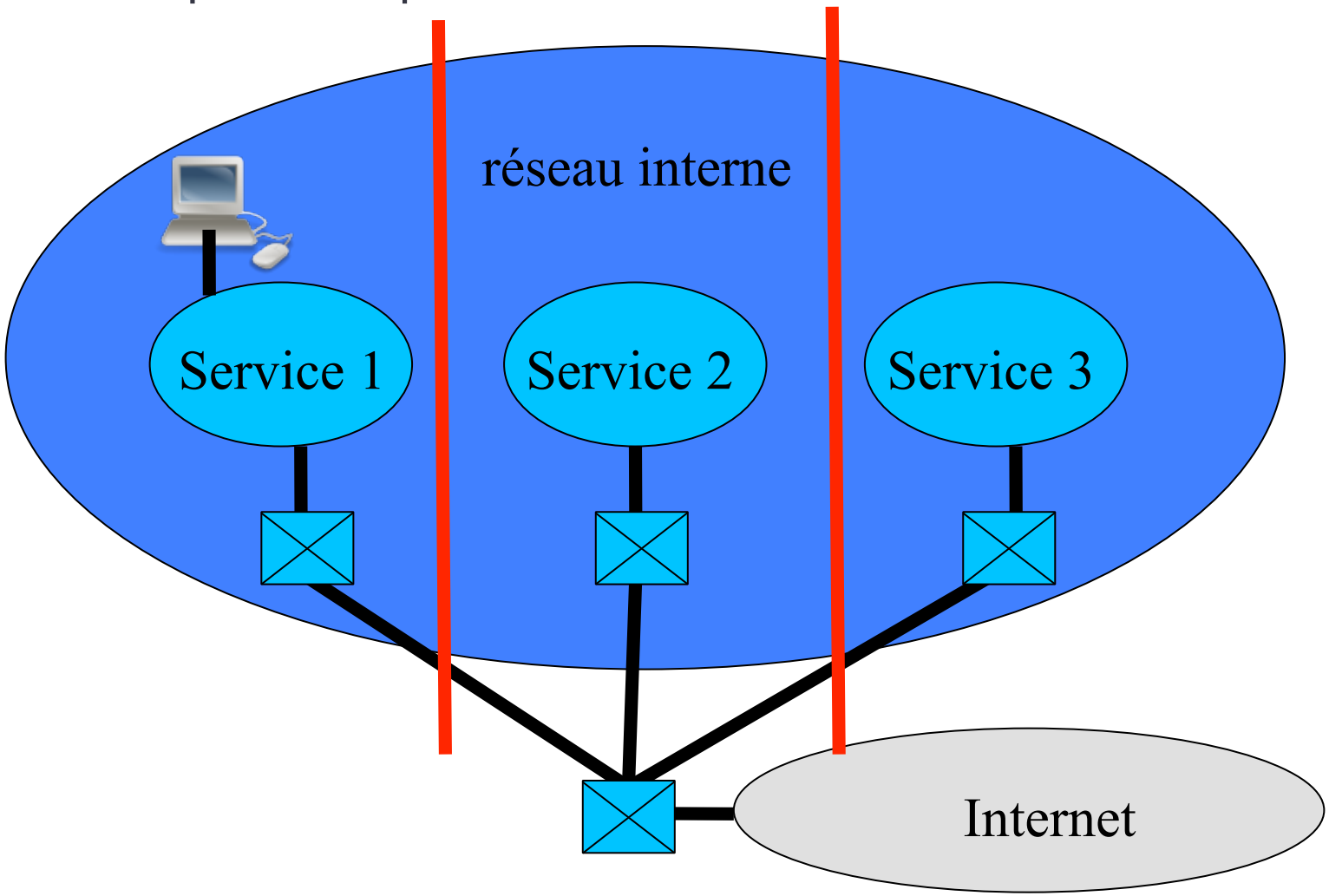
Introduction

- Principe : contrôle des flux entrants et sortants
  - Pare-feu + filtrage



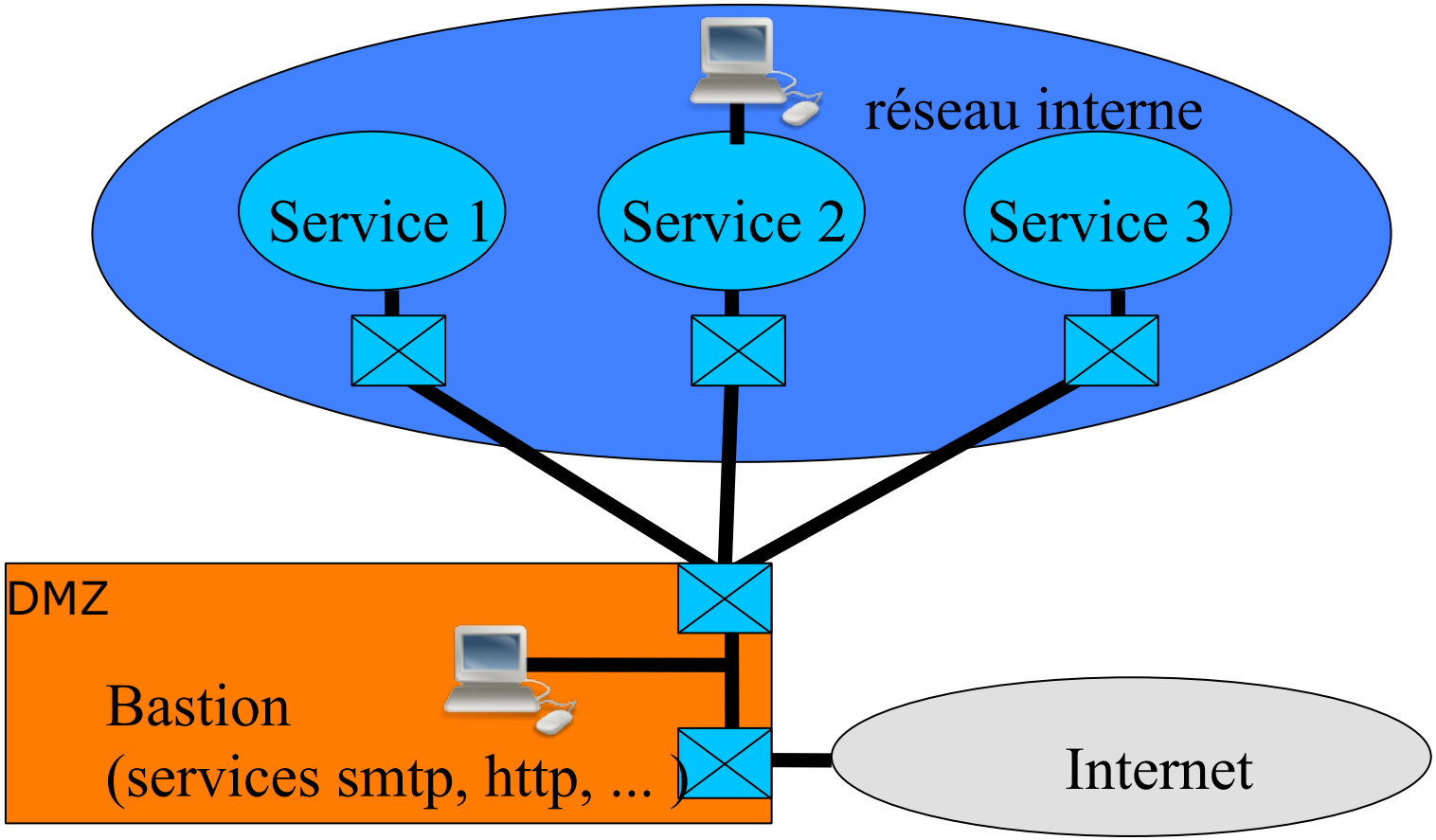
Introduction

- Principe : segmentation du réseau interne
  - → VLAN par exemple



Introduction

- Principe
  - services externes (SMTP, HTTP, ...) gérés à part



Éléments

- Protection
  - Firewall
    - filtrage
  - Bastion
    - Proxy / mandataire
    - (NAT)
  - VPN
  - Cryptage
    - IPSec
- Détection
  - IDS
  - pot de miel

Définitions

- Firewall
  - composant(s) restreignant l'accès entre un réseau protégé (interne) et un autre ens. de réseaux (extérieur).
- Bastion
  - composant hautement sécurisé constituant le principal point de contact entre les hôtes du réseau protégé et l'extérieur.
- Réseau périphérique
  - couche supplémentaire de sécurité ajoutée entre un réseau protégé et l'extérieur
- Proxy : serveur intermédiaire (mandataire)
  - relayer requêtes/réponses approuvées entre un client et un serveur.
- Filtrage de paquets :
  - routage sélectif (autorisation/rejet) de paquets entre des hôtes internes & externes

Pare-feu

- Firewall (pare-feu) doit
  - Empêcher la propagation d'une attaque
  - Laisser passer le trafic utile
- Constitué d'un ou de plusieurs équipements
  - Routeur, machine

Pare-feux

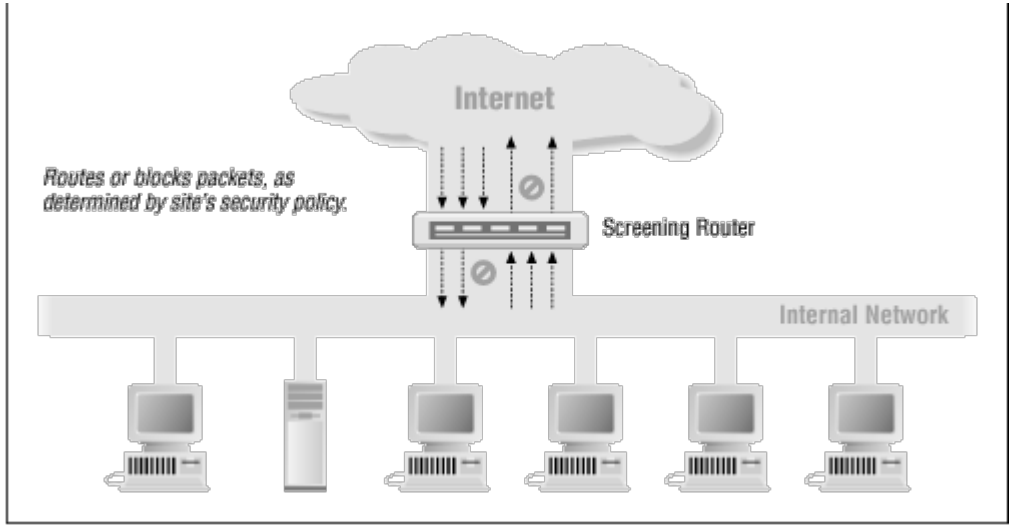
- Firewall (pare-feu) doit
  - Empêcher la propagation d'une attaque
  - Laisser passer le trafic utile
- Typologie
  - Un ordinateur avec logiciel firewall
    - Checkpoint firewall-1, Raptor, Gauntlet, IP-tables
  - Machine avec au – 2 interfaces (routage) + logiciel firewall
  - Matériel = routeur + logiciel firewall
    - Cisco PIX, Cisco IOS, Nokia Checkpoint FW1, WatchGuard, Sonicwall
  - Ordinateur vs Routeur
    - Les firewalls logiciels, attention à la vulnérabilité des OS
    - Routeur : attention à la performance des matériels (processeur, mémoire...)

Pare-feux (II)

- Sans mémoire (stateless)
  - = Ne se rappelle pas des paquets
  - Filtrage sur la trame IP courante
  - Problème : attaque par fragment de paquet
- A mémoire (stateful)
  - = Garde une trace des paquets qui passent
  - Reconstruit l'état de chaque connexion, de certains protocoles
  - filtrage sur le flux
    - + coûteux

Filtage

- Le filtrage sert à limiter le trafic aux services utiles



- Critères de filtrage
  - IP src et #port src et IP dest. #port scr
  - Protocoles (TCP, UDP, ICMP, &)
  - Flags et options (syn, ack, ICMP message type, ...)

Filtrage

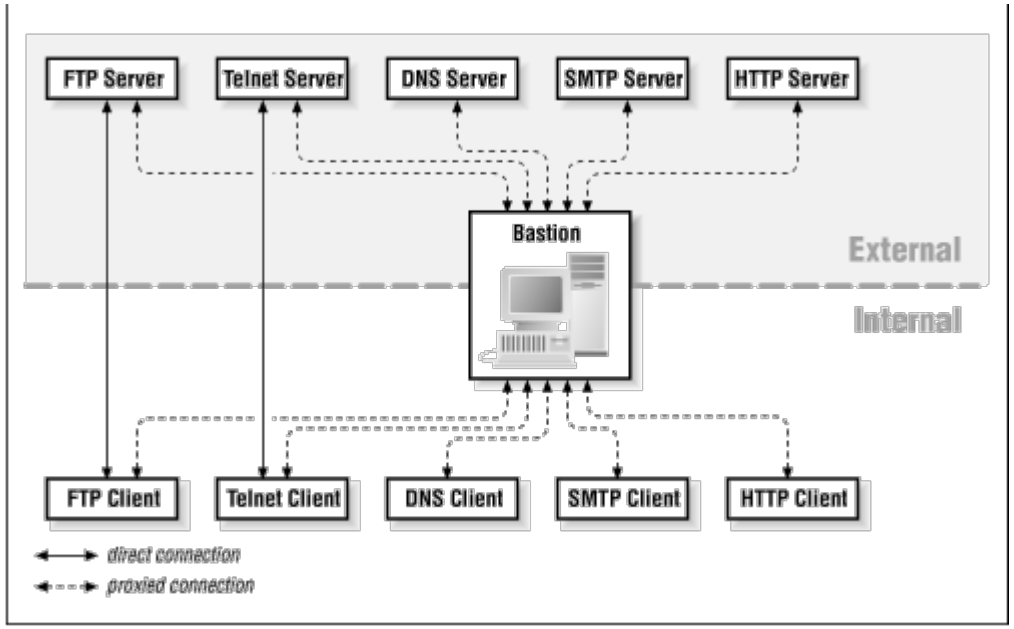
- Exemple
  - Bloquer les connections entrantes sauf pour les connexions SMTP (mail) et HTTP (web) destinées aux serveurs mail et web internes
    - filtrage sur IP et port du destinataire
  - Bloquer certaines IP sources, certains domaines
    - SPAM
  - Autoriser la sortie du mail provenant des serveurs de mail
    - les serveurs de mail sont des IP connues
  - Bloquer les protocoles dangereux comme RPC, X, TFTP...

Routeur vs Pare-feu

- Routeur
  - Fonction de routage
    - Regarde l'IP de destination et sélectionne la meilleure interface pour envoyer le paquet à destination
      - le routeur sait où envoyer le paquet
      - ou le routeur ne sait pas envoyer le paquet (retourne une erreur du type « unreachable destination » à la source.
  - Pare-feu : Routeur + filtre
    - Fonctionne comme un routeur (sélection de l'interface de sortie)
    - + regarde s'il doit ou pas faire sortir le paquet
      - règles de filtrage
    - Placer entre le réseau interne et l'internet, le filtrage assure une part importante de la sécurité

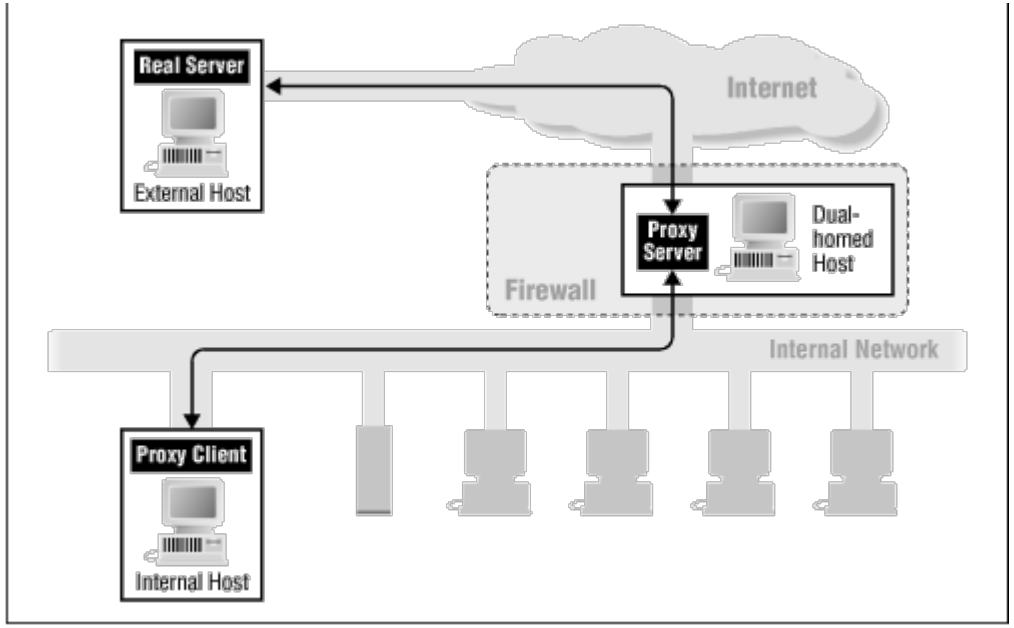
Bastion

- Fournit les services pour communiquer avec l'Internet
  - ex: DNS, SMTP, IMAP, HTTP
  - Fonction : Mettre que les services nécessaires à disposition
  - Note : si un service est compromis alors tous les services du bastion seront aussi considérés compromis



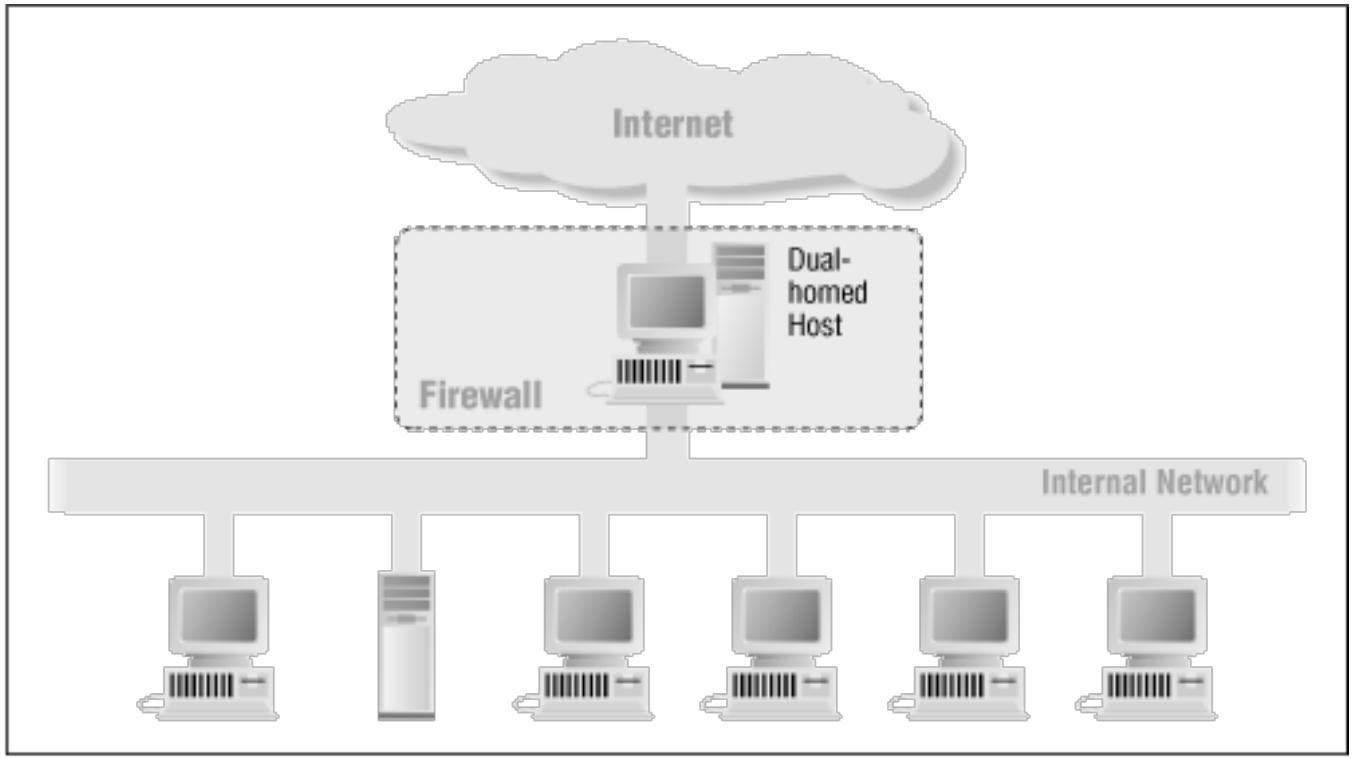
Mandataire

- Mandataire = Proxy
  - Relais applicatif entre un client interne et un service externe
  - Relayer l'information
    - donne l'illusion de parler directement avec le serveur
    - plus ou moins transparent
  - Fonctions : cache, filtre applicatif, modification du contenu...



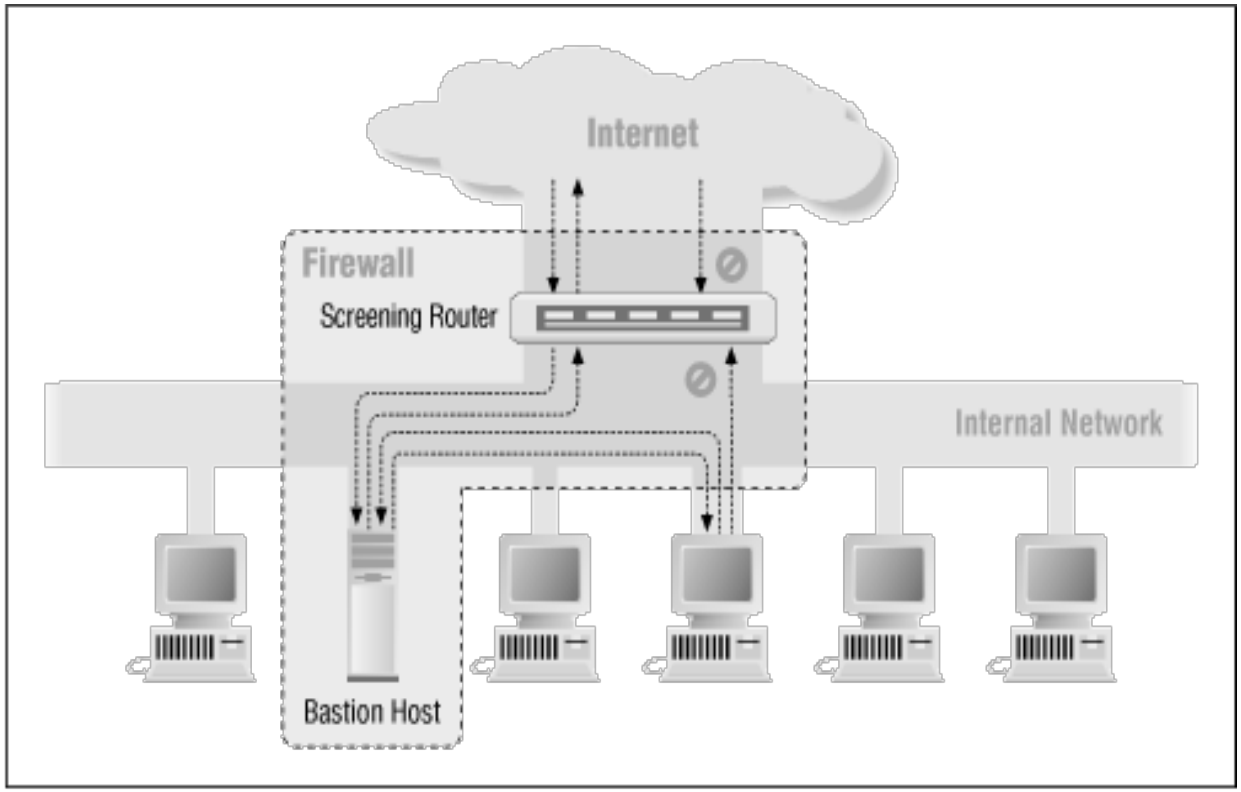
Architecture à double interface

- Une machine avec 2 interfaces
  - = 2 réseaux, contrôle des informations lors du routage
  - Pas de trafic directe entre les réseaux interne & externe
  - Que des services par mandatement
  - Si l'hôte est attaqué avec succès, le réseau interne est accessible !



Architecture d'hôte à écran

- Routeur + filtrage
  - Renvoyer tout trafic autorisé de l'extérieur vers le bastion
    - Bastion = le seul point de contact entre les réseaux interne & externe
- Trafic entre machines internes & routeur-écran interdit
- Filtrage des connexions entre machines internes & l'extérieur

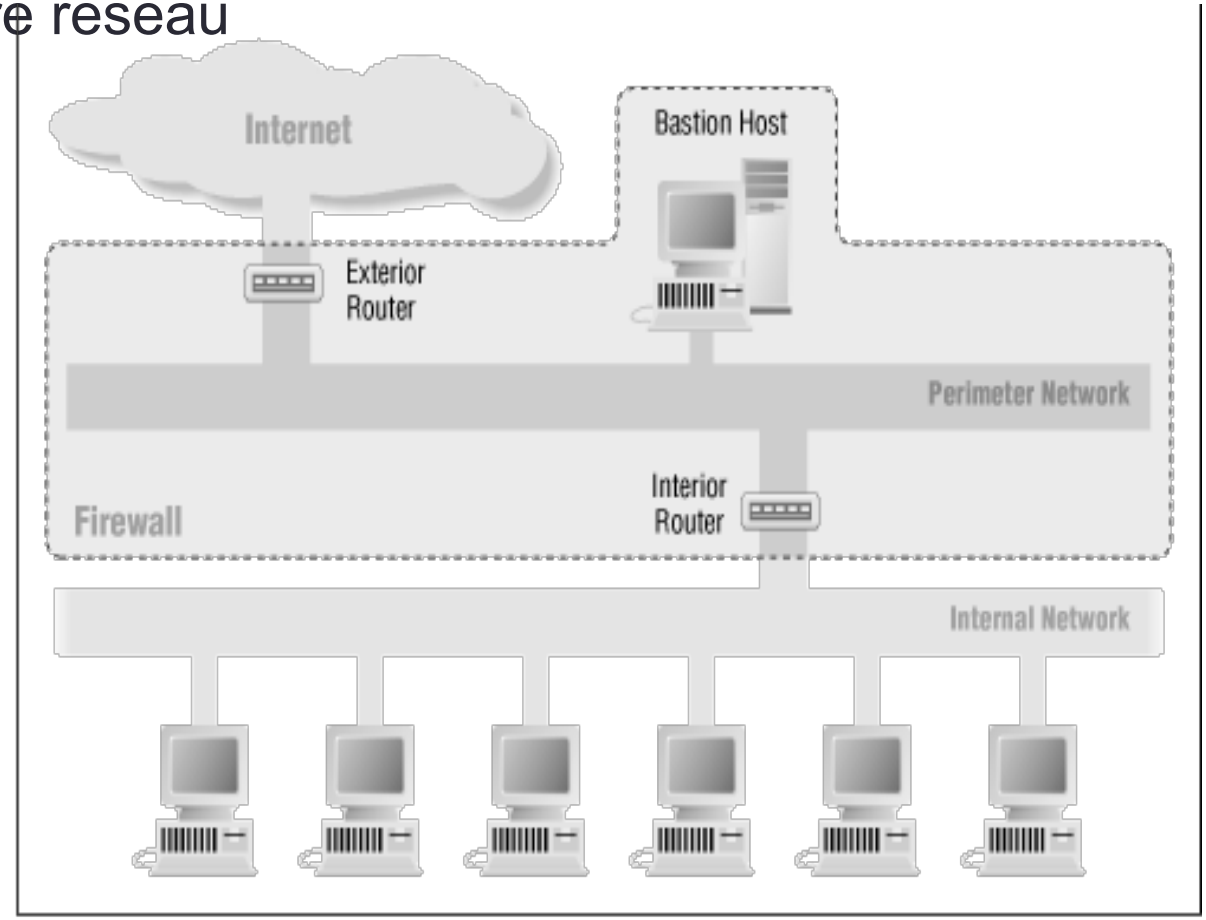


Architecture d’hôte à écran

- Avantages :
  - Plus facile de protéger un routeur qu’une machine
  - Meilleure facilité d’utilisation
- Inconvénients :
  - Bastion présent sur le réseau interne
  - Routeur = point unique de défense !
  - Si le routeur ou le bastion sont attaqués avec succès, l’intégralité du réseau interne est directement accessible

Architecture de sous-réseaux à écran

- 2 routeurs + Bastion
- 3 réseaux
  - Bastion dans son propre réseau



Architecture de sous-réseaux à écran

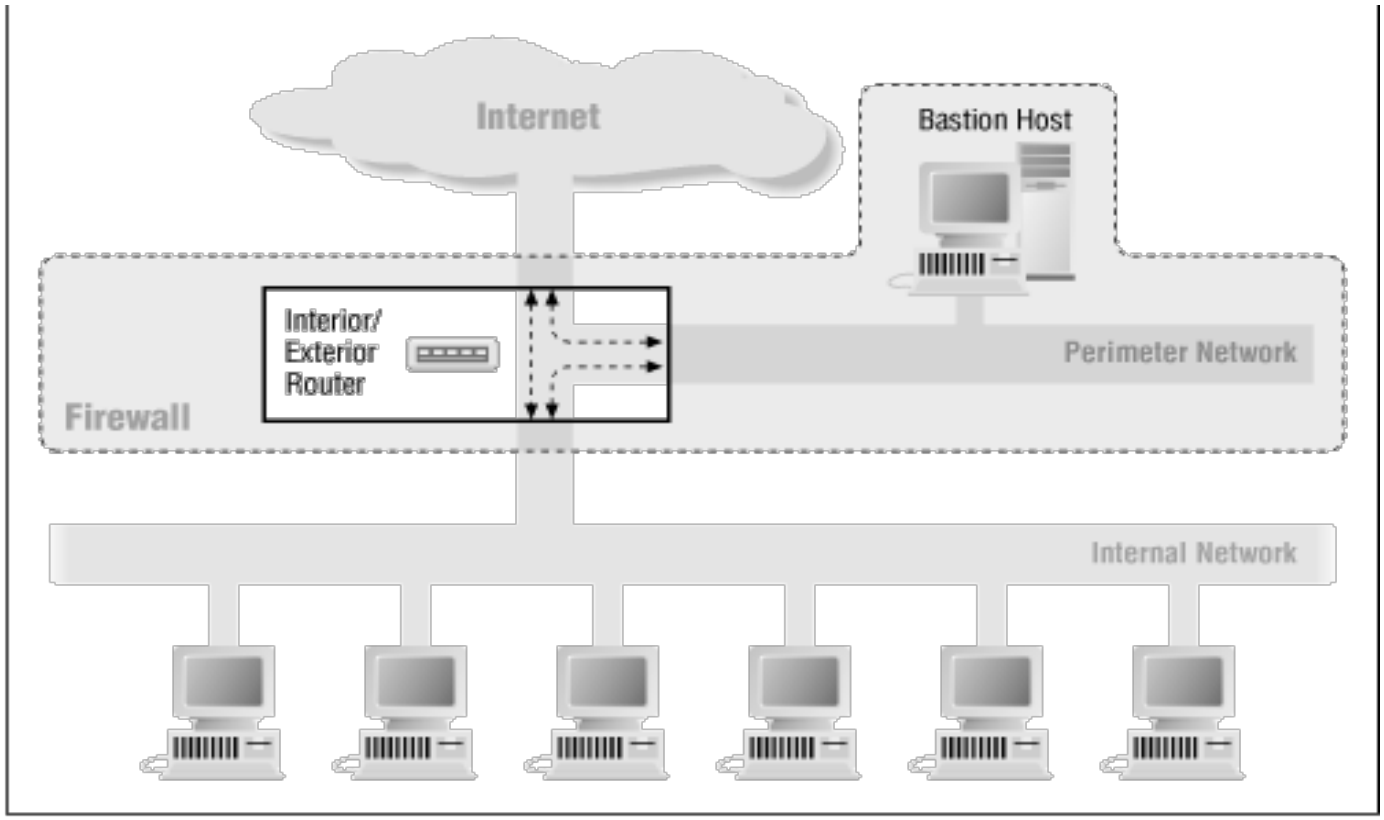
- Rôle du bastion :
  - Principal point de contact pour l'extérieur
  - Utilisé en tant que serveur mandataire
- Routeur interne (routeur goulet) :
  - Protection du réseau interne vis-à-vis de l'extérieur et du réseau périphérique
  - Essentiel du FP du firewall : permettre à des services sélectionnés de sortir du réseau interne vers l'extérieur (sans mandatement)
  - Limitation des services autorisés entre le bastion et le réseau interne (routage vers serveurs dédiés)

Architecture de sous-réseaux à écran

- Routeur extérieur (routeur d'accès) :
  - En théorie : protection du réseau périphérique & réseau interne
  - En pratique : on tend à laisser tout passer depuis le réseau périphérique et filtre les connexions provenant de l'extérieur pour protéger les machines du réseau périphérique (bastion & routeur interne)
  - Tâche réellement utile : bloquer tout paquet de l'extérieur prétendant provenir de l'intérieur (falsification d'@ machine interne)

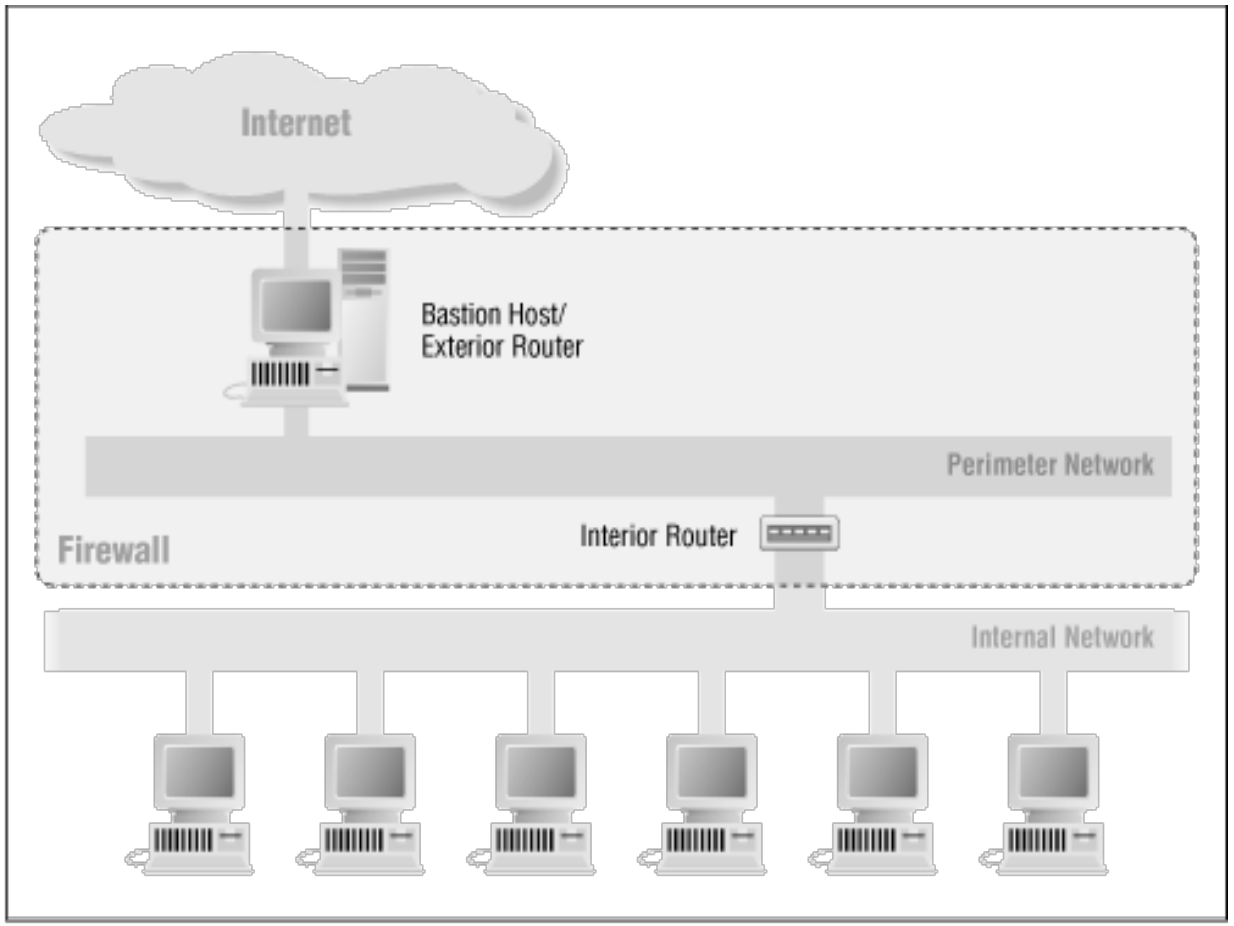
Architecture

- 1 routeur avec 3 interfaces + bastion

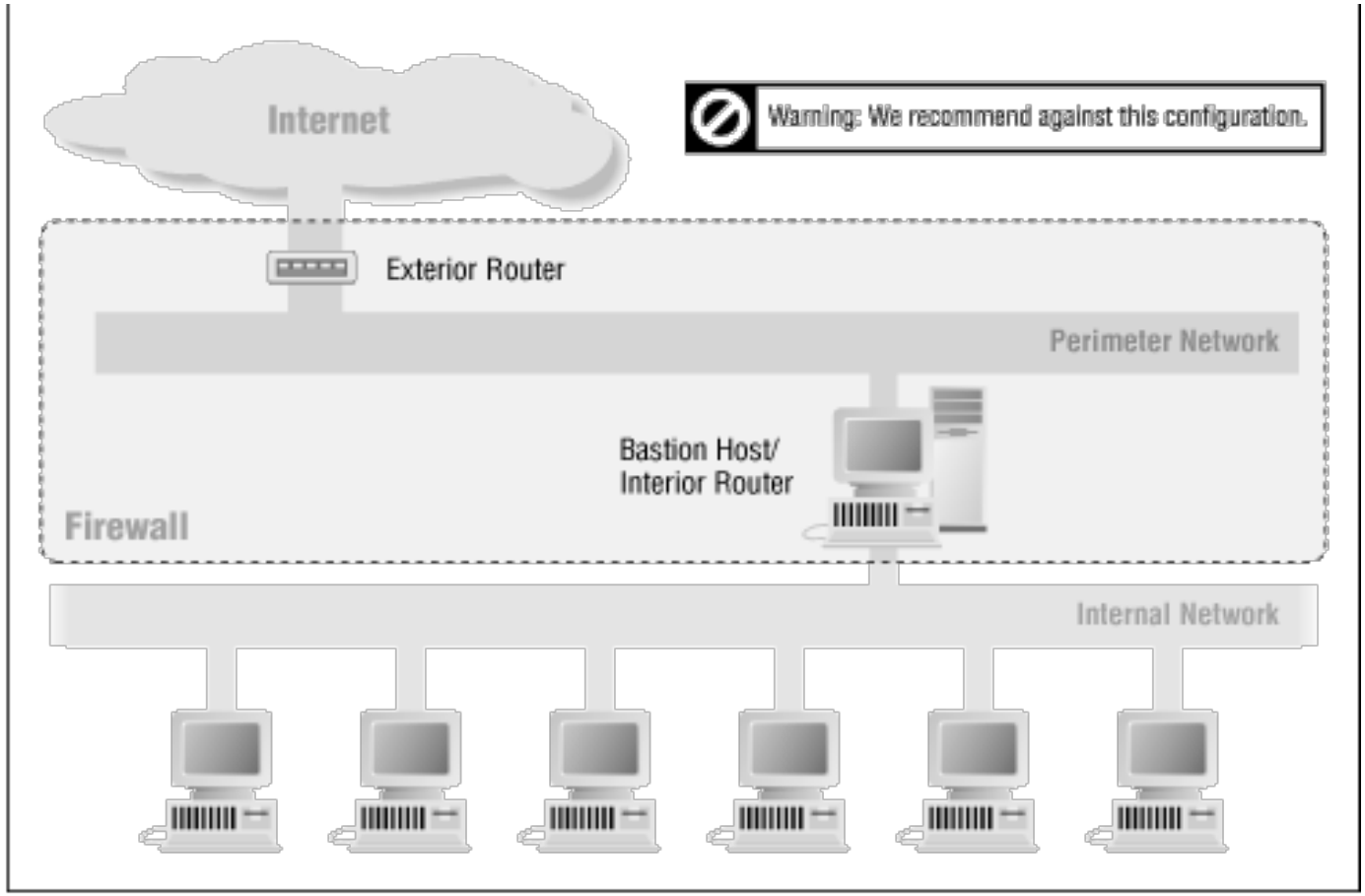


Architecture

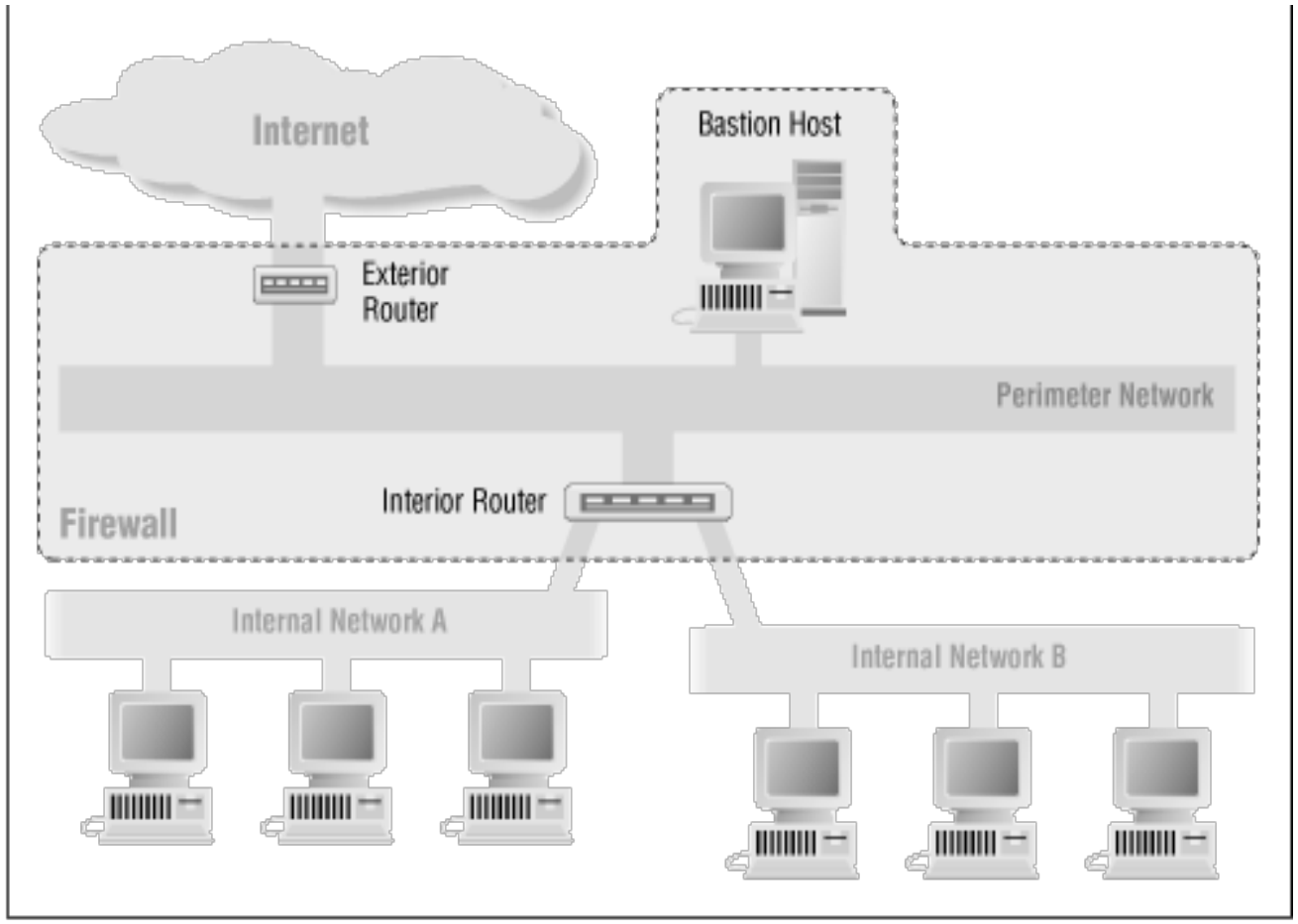
- Structure type
  - Sauf routeur externe + Bastion fusionnés



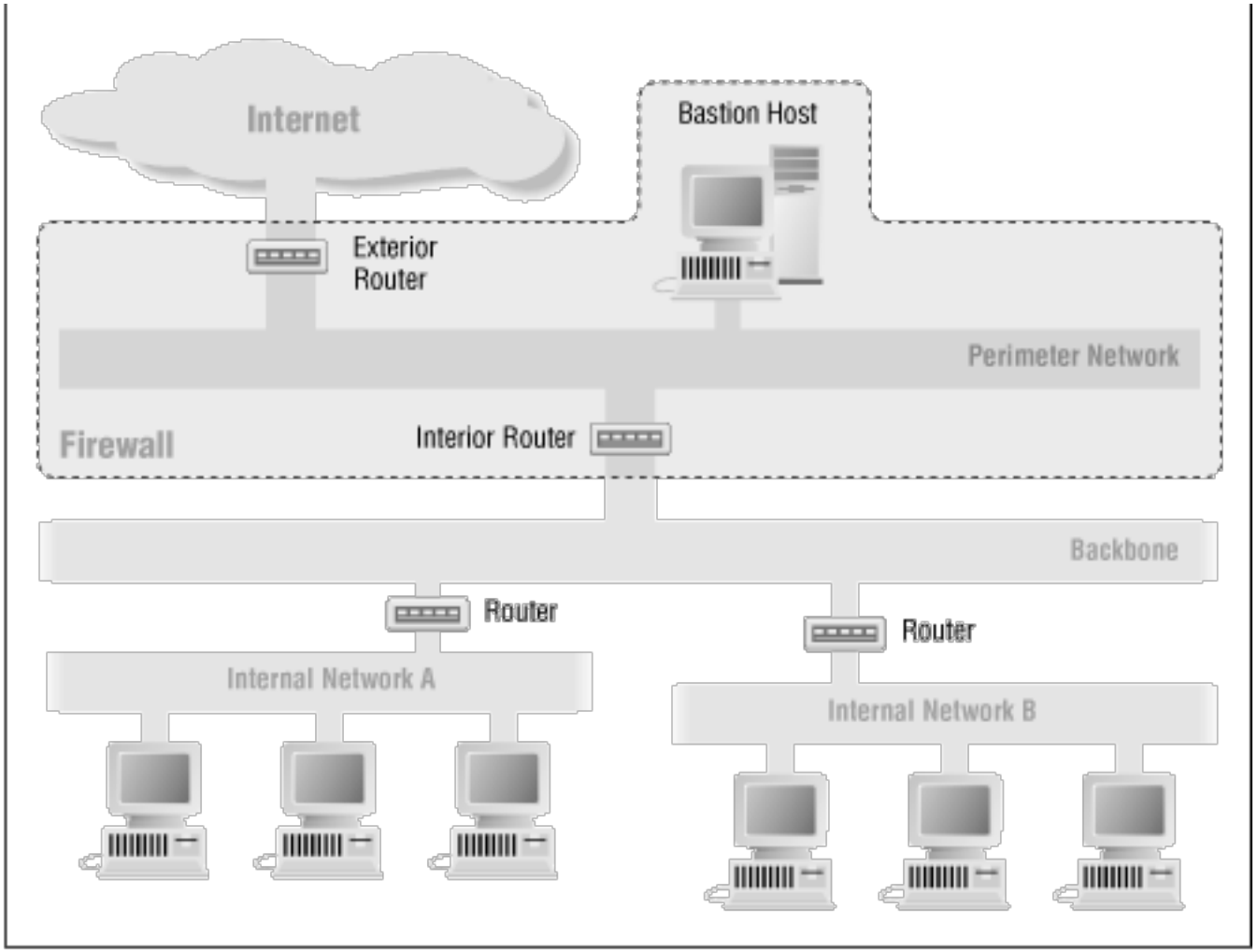
Architecture



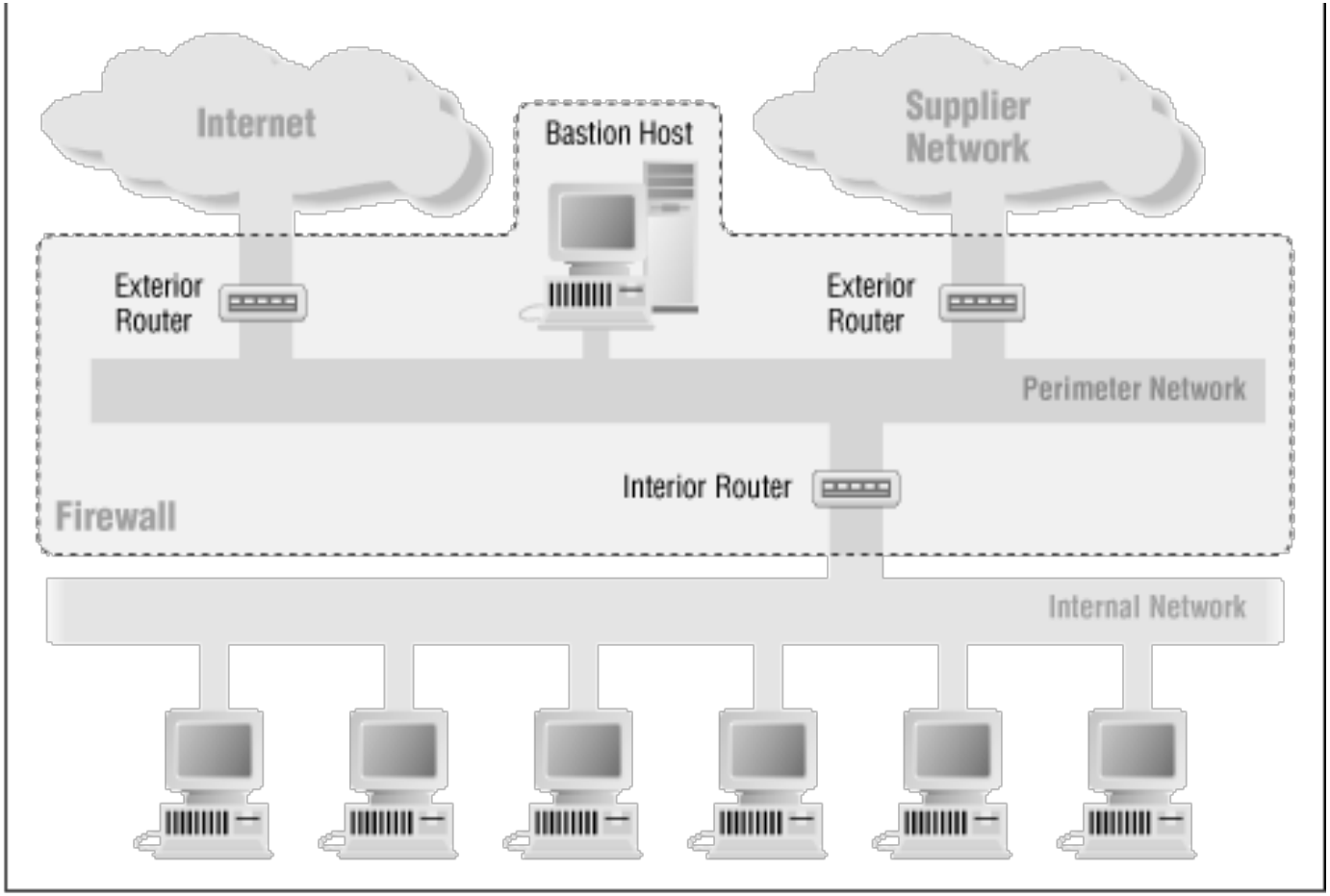
Architecture



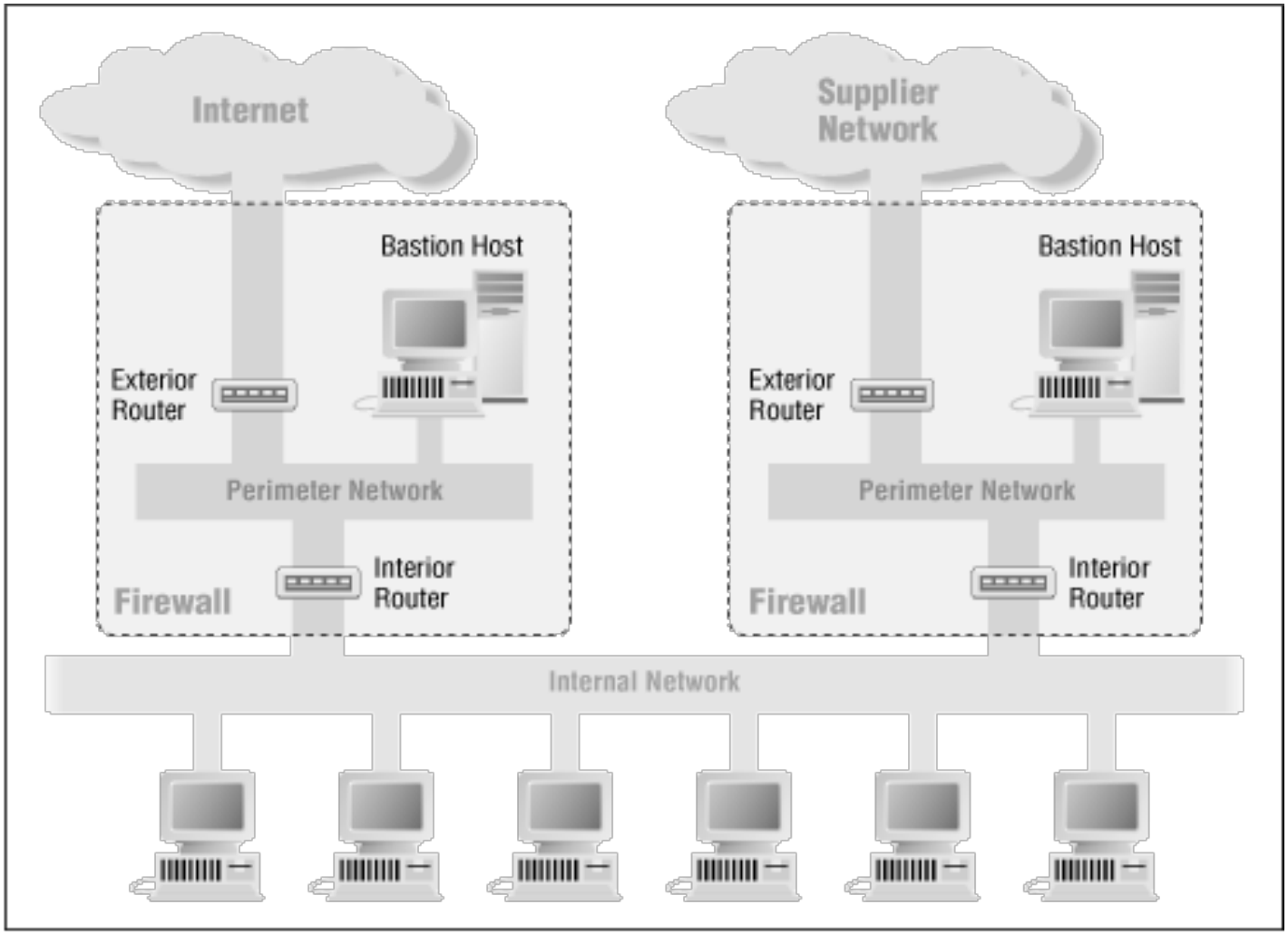
Architecture



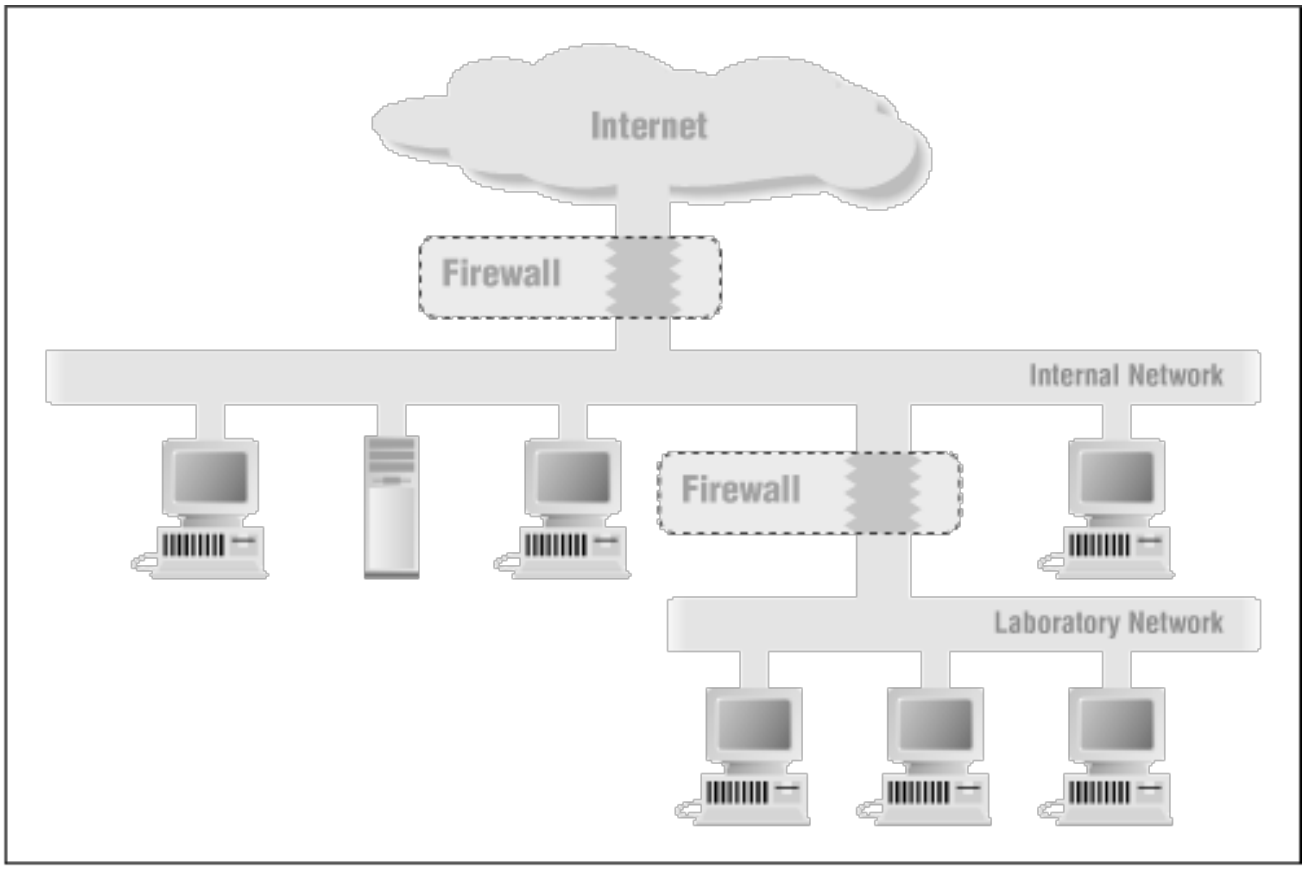
Architecture



Architecture



Architecture



Principe

- Défense en profondeur
  - Eviter que la sécurité dépende d'une mesure unique
    - Plusieurs mesures de sécurité valent mieux qu'une
  - Exemple
    - Antivirus sur les serveurs de messagerie ET sur les postes de travail
    - On sécurise quand même (configuration, patchs)
      - les machines qui sont protégées par un firewall
      - les machines qui n'ont pas d'accès direct à l'Internet
- Simplicité
  - La plupart des problèmes de sécurité sont des erreurs humaines
    - oublis, mauvaise configuration, erreur de manipulation...
  - Dans un système simple :
    - le risque d'erreur est plus petit
    - il est plus facile de
      - comprendre la topologie, son fonctionnement
      - vérifier son bon fonctionnement

Principe

- **Interdire tout ce qui n'est pas explicitement permis**
  - mieux que de permettre tout ce qui n'est pas explicitement interdit
  - Les menaces ne sont pas toutes connues à l'avance
  - En cas d'erreur
    - il vaut mieux interdire quelque chose d'utile que d'autoriser une attaque !
    - les utilisateurs remarqueront le problème
- Périmètres de sécurité
  - Découper le réseau en périmètre de sécurité
  - Regrouper les éléments de même nature
    - définir des niveaux de sécurité
    - faciliter la mise en place des règles de sécurité
      - définir les fonctions des équipements (serveur et services, poste de travail)

Stratégie

- Goulet d'étranglement
  - Etablir les périmètres de sécurité des sous-réseaux
  - Mettre en place les points de passage entre les sous-réseaux
    - établir les règles d'entrée/sortie
- Authentification
  - Vérifier l'identité des utilisatrices, des machines…
  - Lister qui peut passer les points de passage
    - utilisateur, machine, protocole
  - Politique des mots de passe

Stratégie

- Moindre privilège
  - Limiter les privilèges
    - Chaque élément d'un système (utilisateur, logiciel) ne doit avoir que le minimum de privilèges nécessaires pour accomplir sa tâche
  - Exemples:
    - Les utilisateurs normaux ne doivent pas être administrateurs
    - Les administrateurs doivent aussi utiliser des comptes d'utilisateurs
    - Un serveur web tourne sous nobody (pas root)
- Séparation des pouvoirs
  - Définir les responsables des différentes zones de sécurité
  - Séparer et limiter les pouvoirs des responsables
  - Non applicable pour les petites entreprises
    - 1 ou 2 responsables informatiques

Stratégie

- Confidentialité des flux réseau
  - Applicable pour les données sensibles
    - Pour les communications intersite / interréseaux transitant sur des réseaux publics
    - Identifier les données, mesurer l'impacte en cas de perte/vole/ divulgation
  - Chiffrer si elles contiennent des données confidentielles
- Antivirus : Contrôler tout vecteur de propagation de virus
  - vecteurs
    - média amovibles (disquette, CD, clé USB)
    - email, navigateur internet (java, JavaScript, activex, téléchargement)
    - utilisateur itinérant

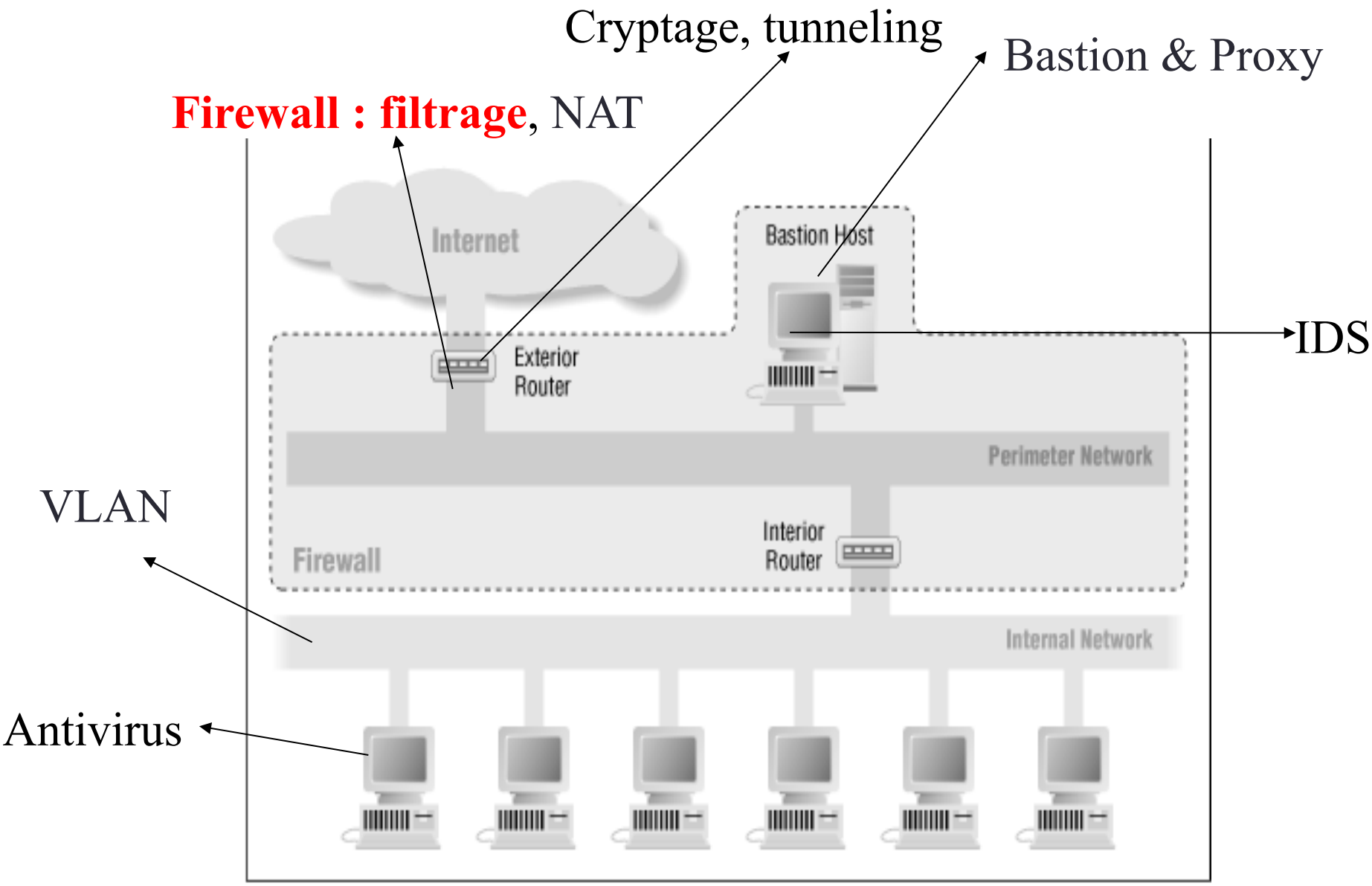
Stratégie

- Participation universelle
  - Un système de protection n'est efficace que si tous les utilisateurs le supportent
    - But : firewall est d'autoriser tout ce qui est utile en évitant les dangers
    - Système trop restrictif pousse les utilisateurs à devenir créatifs
    - Connaître les besoins des utilisateurs et communiquer les raisons des restrictions (mesures et risque)
  - Exemples :
    - verrouiller/éteindre les stations de travail lorsqu'elles ne sont pas utilisées
    - contrôle des personnes physiques / fermeture des zones sensibles
    - mots de passe

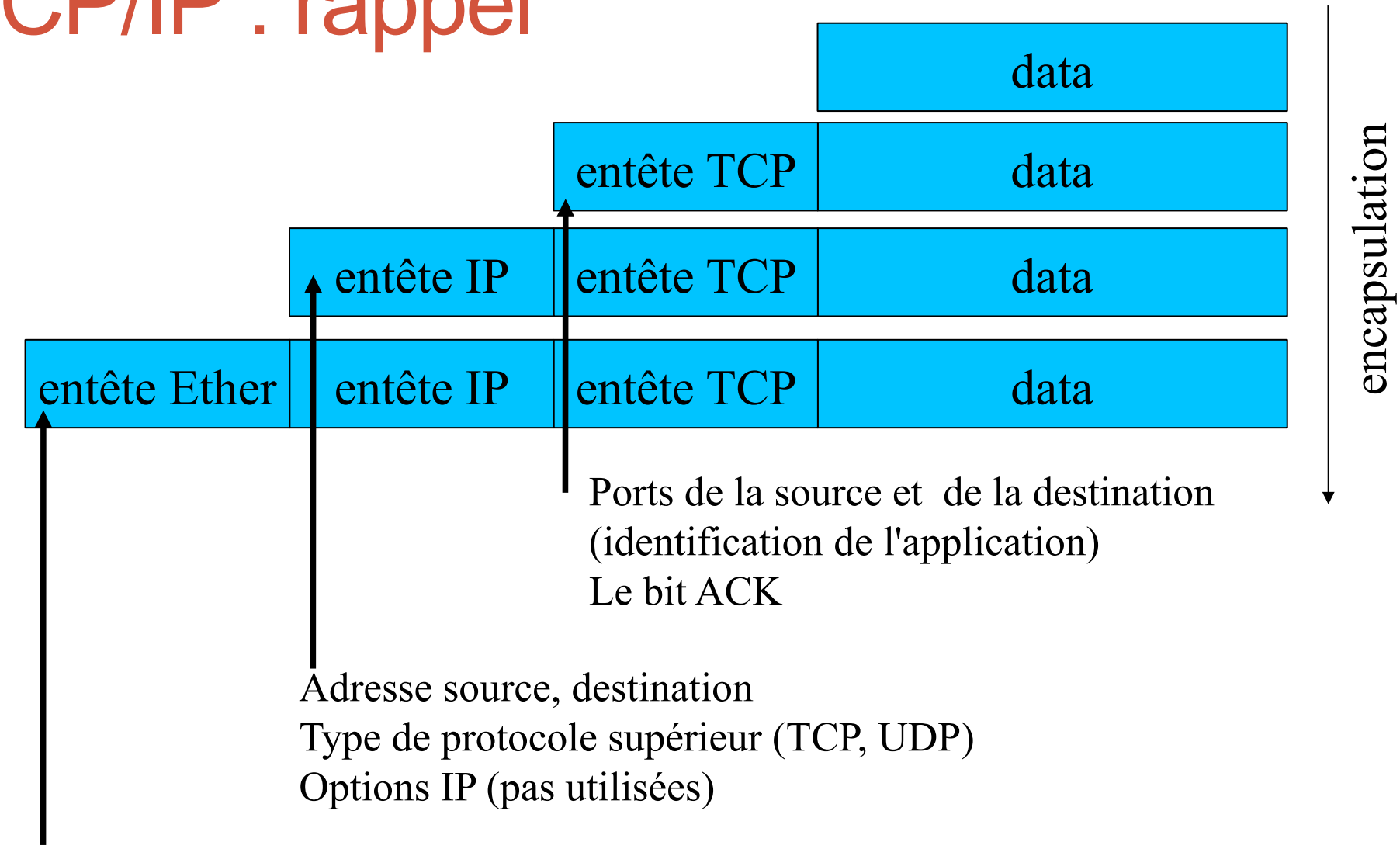
Stratégie

- Contrôle régulier
  - Objectif : valider la politique de sécurité
  - Simuler des tentatives de pénétration
    - audit sécurité
  - Appliquer à tous des aspects de l'entreprise
    - documentation
    - topologie réseaux, matériels, logiciels, OS
    - sécurité physique

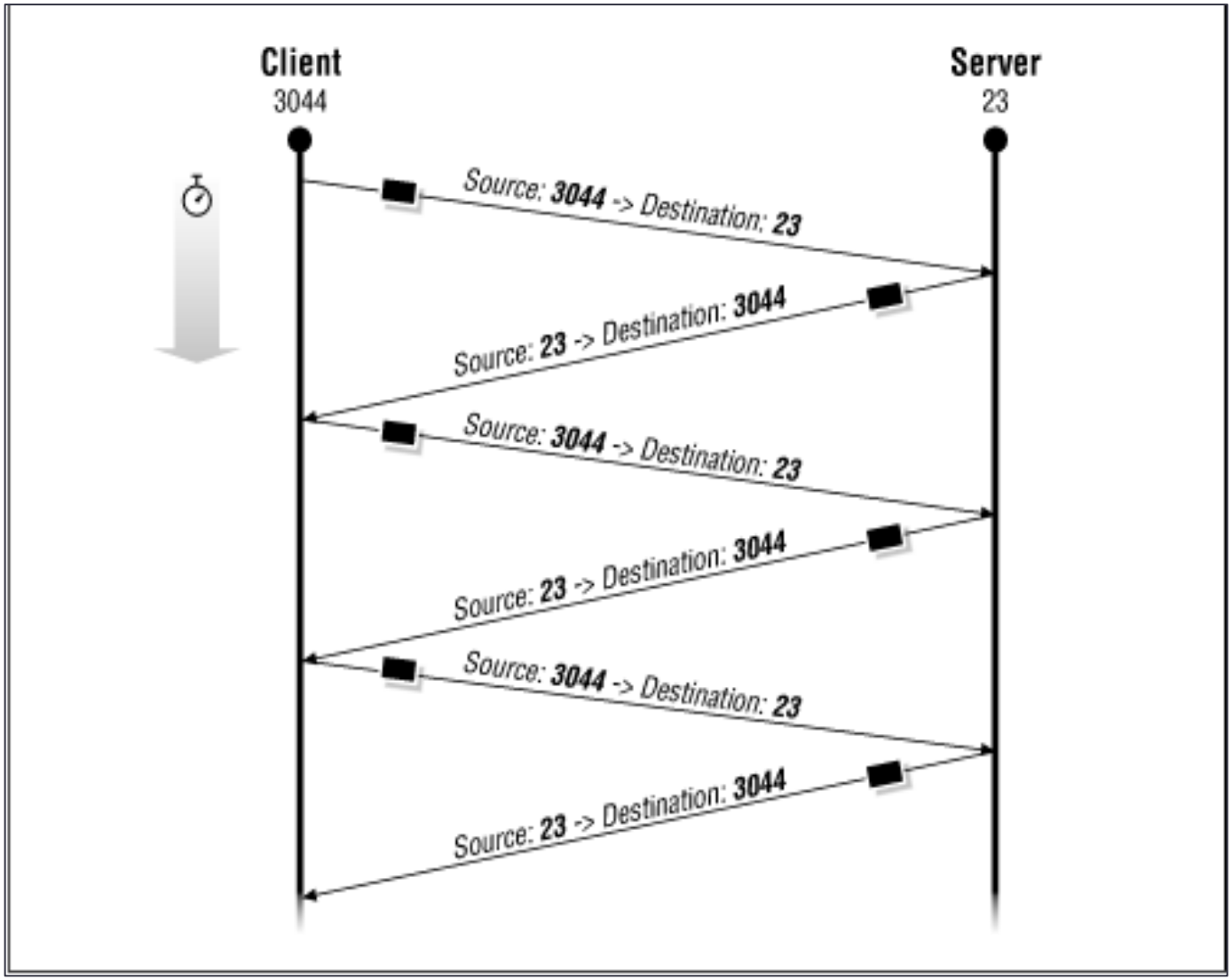
Filtrage


Cryptage, tunneling
Bastion & Proxy
Firewall : filtrage, NAT
Internet
Bastion Host
IDS
Exterior Router
Perimeter Network
VLAN
Interior Router
Firewall
Internal Network
Antivirus

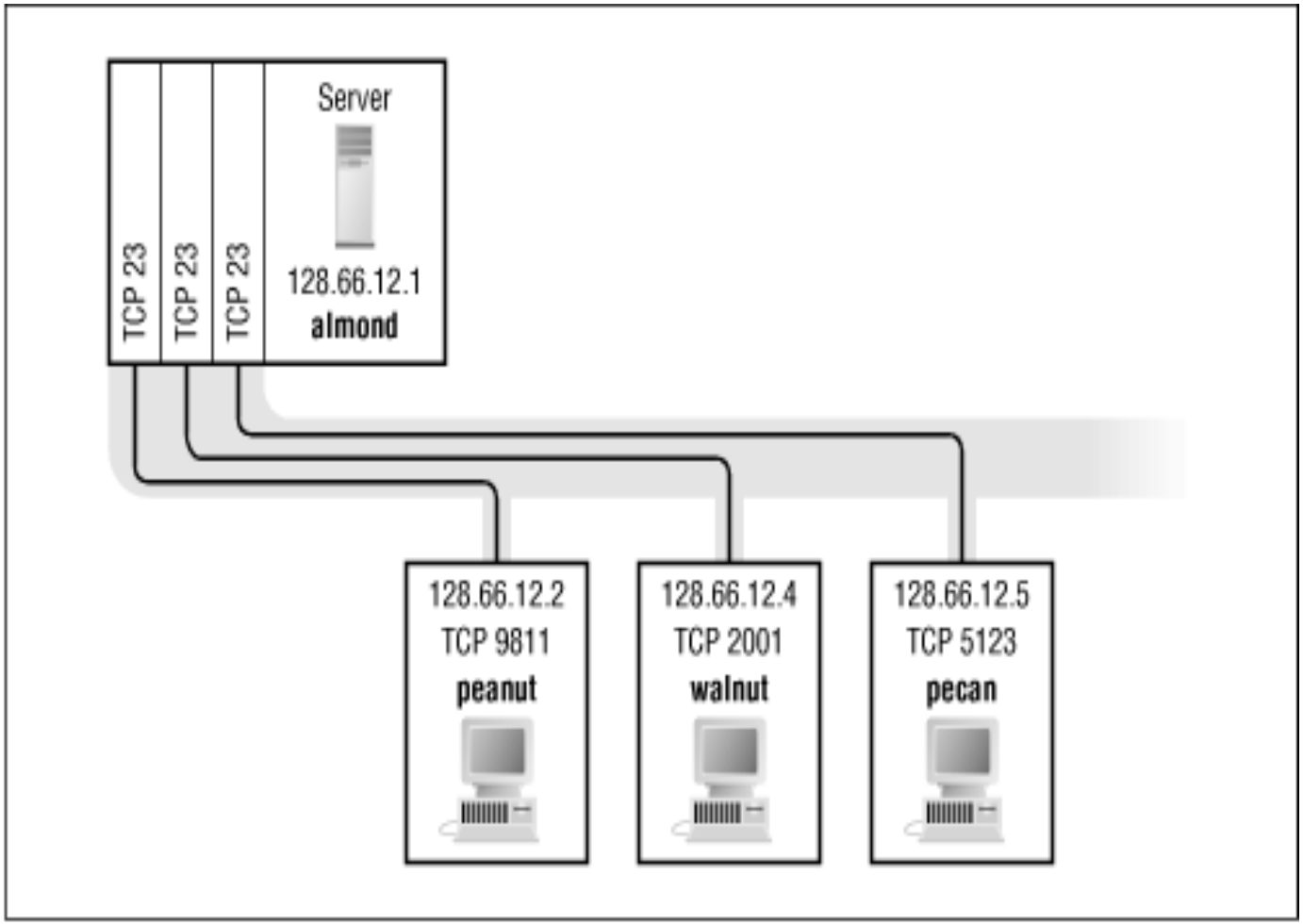
TCP/IP : rappel



TCP/IP : client / serveur



TCP/IP : couples (@IP / #ports)



TCP/IP : protocoles

Service		Protocole	Source	Destination
DNS (lookups)		TCP/UDP	X>1023	53 (clients--> serveurs)
DNS			53	53 (serveur--> seveur)
SMTP	demande	TCP	X>1023	25
SMTP	réponse	TCP	25	X
HTTP	demande	TCP	X>1023	80 (souvent)
HTTP	réponse	TCP	80	X
POP	demande	TCP	X>1023	110
POP	réponse	TCP	110	X

Filtrage : principe

- Laisser passer ou non un paquet
- Repose sur les adresses IP
  - Doivent être correctes (pas truquées).
  - → vérifier leur cohérence en entrée (depuis l'extérieur comme l'intérieur)
- Repose sur des règles
  - Si un paquet ne satisfait pas les règles
    - "drop" : un message de log si violation des règles
      - peut générer beaucoup de log, qui va regarder ?
    - Faut-il renvoyer un ICMP (erreur) ?
      - NON, pourrait aider les "pirates" à comprendre la politique sécurité du site.
  - Différencier IN de OUT
  - Attention l'ordre des règles est important

Filtrage : fonctionnement

- Repose sur un ensemble de règles
  - Autoriser la connexion (permit/allow)
  - Bloquer la connexion (deny)
  - De rejeter la demande de connexion sans avertir l'émetteur (drop)

- Permettre de mettre en oeuvre le filtrage
- Filtrage dépendant de la politique de sécurité
- 2 politiques :
  - Empêcher les échanges qui ont été explicitement interdits
  - Autoriser uniquement les communications ayant été explicitement autorisées :
    - "Tout ce qui n'est pas explicitement autorisé est interdit"
    - + sûre, + difficile et contraignante

Filtrage simple

- Filtrage simple = « stateless packet filtering »
  - Analyse des en-têtes de chaque paquet de données (datagramme)
- Données utiles :
  - adresse IP de la machine émettrice
  - adresse IP de la machine réceptrice
  - type de paquet (TCP, UDP, etc.)
  - numéro de port de destination ou de source
    - Identification du service

Filtage simple : exemple

Règle	Action	IP source	IP dest	Protocol	Port source	Port dest
1	Accept	192.168.10.20	194.154.192.3	tcp	any	25
2	Accept	any	192.168.10.3	tcp	any	80
3	Accept	192.168.10.0/24	any	tcp	any	80
4	Deny	any	any	any	any	any

Filtrage dynamique

- Filtrage dynamique : « stateful packet filtering »
- Filtrage simple
  - examiner les paquets IP indépendamment les uns des autres
  - ne gère pas la notion de session (TCP)
    - s'assurer le bon déroulement des échanges
  - Problème des ports dynamique (ftp)
- Besoin :
  - inspection des couches 3 et 4 d'OSI
  - Effectuer un suivi des transactions entre le client et le serveur

- Assurer un suivi des échanges
  - = tenir compte de l'état des anciens paquets pour appliquer les règles de filtrage
- Plus performant que le filtrage simple

Filtrage applicatif

- Filtrage applicatif =
  - « passerelle applicative » (ou « proxy »)
- Permet de filtrer les communications application par application
  - opère donc au niveau 7 (couche application) du modèle OSI
  - suppose une connaissance des protocoles
  - Propre à chaque application

- Proxy : un intermédiaire entre les machines du réseau interne et le réseau externe
- But : subir les attaques à la place des postes clients
- Peut potentiellement avoir une vulnérabilité
  - recommander de dissocier le pare-feu et proxy

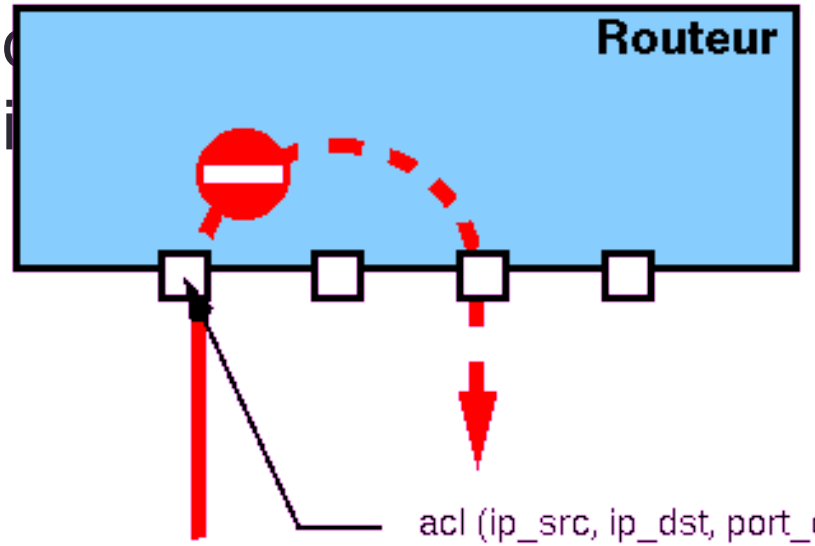
FILTRAGE IOS CISCO

Routeur CISCO : ACL

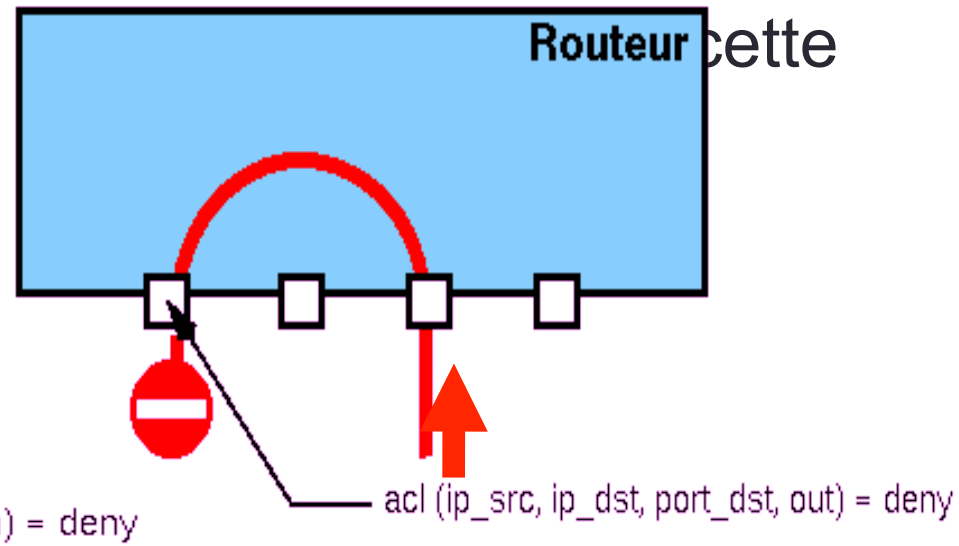
- Les ACL (Access Control Lists), IOS CISCO
  - instructions qui expriment une liste de règles
  - régles appliquées à chaque paquet IP transitant à travers le routeur et qui ont pour paramètres :
    - l'adresse IP de l'émetteur du paquet
    - l'adresse IP du destinataire du paquet
    - le type du paquet (tcp, udp, icmp, ip)
    - le port de destination du paquet
  - Pour un paquet donné, l'ACL rend deux valeurs
    - deny : le paquet est rejeté
    - permit : le paquet peut transiter par le routeur
  - On associe à chaque interface du routeur une ACL avec le sens du trafic

Routeur CISCO

- ACL de type in
  - contrôle le trafic qui entre



- ACL de type out
  - contrôle le trafic qui



Attention : les ACL ne s'appliquent qu'au trafic en transit et pas au trafic généré par le routeur lui-même.

Par ex., une connexion Telnet vers le routeur n'est pas soumise aux ACL.

Routeur CISCO : numéro d'ACL

- 5 catégories :
  - <1-99> IP standard access list
    - Ne permettre d'utiliser que les adresses sources pour identifier les paquets
  - <100-199> IP extended access list
    - Permettre d'identifier un paquet par les adresses IP, protocoles et ports de la source et de la destination
  - <200-299> Protocol type-code access list
    - Filtrage sur le protocole
  - <700-799> 48-bit MAC address access list
    - Filtrage sur adresse MAC source
  - <1100-1199> Extended 48-bit MAC address access list
  - d'autres types existent :
    - pour les autres protocoles qu'IP

CISCO : Les listes de contrôle d'accès standard

- Permettre d'autoriser ou d'interdire
  - des adresses spécifiques
  - un ensemble d'adresses
  - ou de protocoles

- Créer par la commande suivante :
  - access-list numéro_de_liste_d'accès {permit | deny} source {masque_source}
- Avec
  - Numéro_de_liste_d'accès : identifie la liste
  - permit | deny : autoriser ou interdire
  - Source : identifie l'adresse IP source
  - Masque_source : bits de masque générique

- Exemple :
  - Access-list 1 deny 172.69.0.0 0.0.255.255

CISCO : listes de contrôle d'accès étendues

- Permettre de faire un filtrage plus précis :
  - IP source destination
- Créer par la commande suivante :
  - Access-list numéro_de_liste_d'accès {permit | deny} protocole source {masque_source} destination {masque_destination} {opérateur opérande} [established] [log]

  - Avec
    - Numéro_de_liste_d'accès : identifie la liste
    - Permit | deny : autoriser ou interdire
    - Protocol : IP, TCP, UDP, ICMP, GRP, IGRP
    - Source et destination : adresse IP source et destination

CISCO : listes de contrôle d'accès étendues

- Access-list numéro_de_liste_d'accès {permit | deny} protocole source {masque_source} destination {masque_destination} {opérateur opérande} [established] [log]
- Avec (suite)
  - Masque_source et Masque_destination : bits de masque générique
  - Opérateur : (Lt, Gt, Eq, neq) ; Opérande : n° de port
  - Established : autorise le trafic TCP si les paquets utilisent une connexion établie (bit de ACK)
  - Log :
    - permet d'envoyer sur un serveur de type syslog un message à chaque fois qu'un paquet satisfait un élément d'une ACL
    - utile pour les ACL de type "deny"
    - surveillance des tentatives de piratages

CISCO : numéro de port

Décimal	Mot-clé	Description	Protocole
20	FTP-DATA	FTP (données)	TCP
21	FTP	FTP	TCP
23	TELNET	Connexion en mode terminal	TCP
25	SMTP	SMTP	TCP
53	DOMAIN	Serveur DNS	TCP:udp
69	TFTP	Serveur TFTP	UDP
80	http	WWW	TCP

CISCO : assignation d'une ACL

- Une fois la liste de contrôle d'accès crée, il faut
  - L'assigner à une interface de la manière suivante :
    - Router(config-if)#ip access-group numéro_liste_d'accès {in | out }
    - Avec
      - in | out : appliquée pour le trafic entrant ou sortant

- Pour vérifier les listes de contrôle d'accès
  - show ip interface
  - show access-lists
    - affiche le contenu des ACL
    - Avec le numéro en option :
      - consulter une liste spécifique

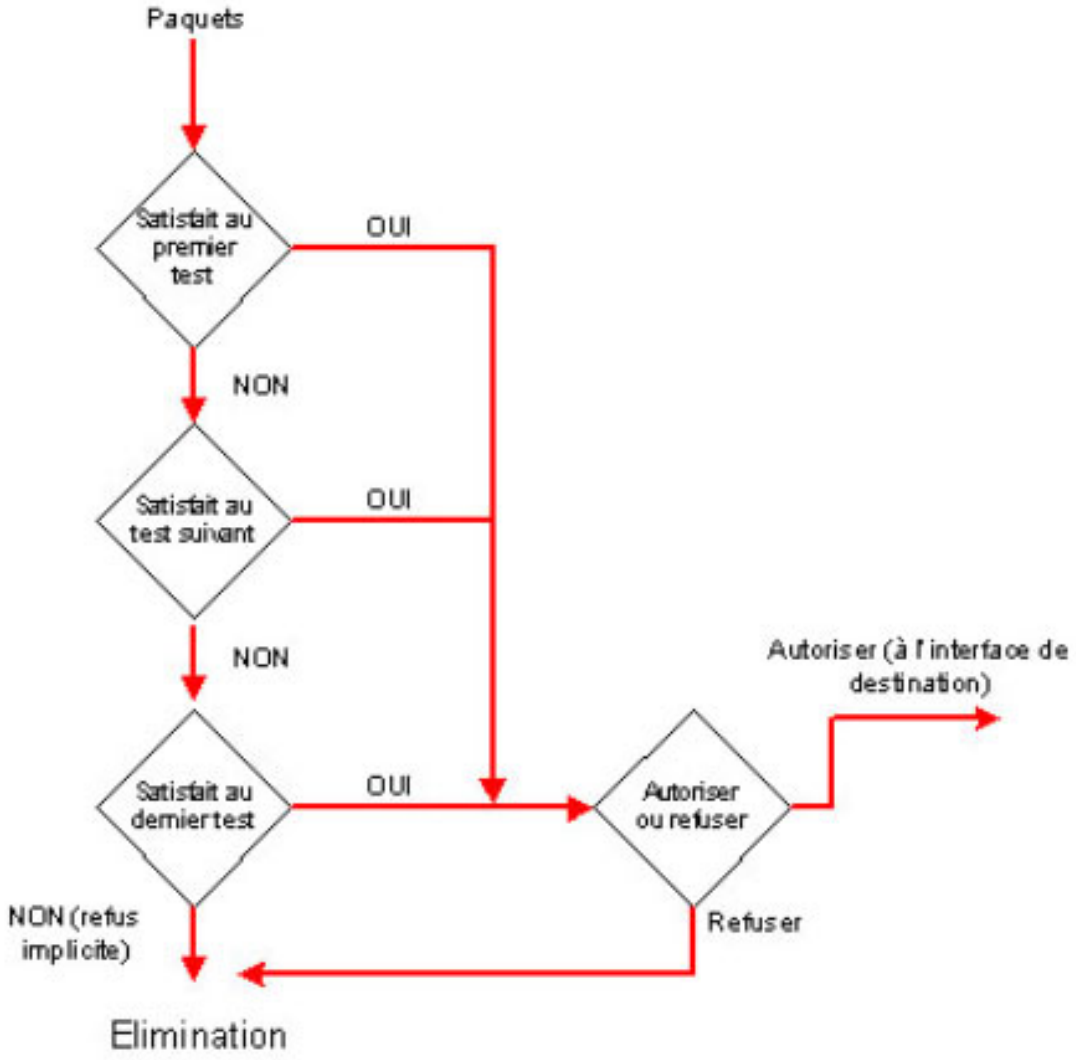
CISCO : emplacement des ACL

- Ou placer les ACL :
  - ACL étendues
    - →le plus près possible de la source du trafic refusé
  - ACL standard
    - → le plus près possible de la destination

- Routeurs périphériques
  - situés aux frontières du réseau
  - Au moins deux listes (eth in et out)
  - Fournir une protection de base
- Faire des ACL par protocole

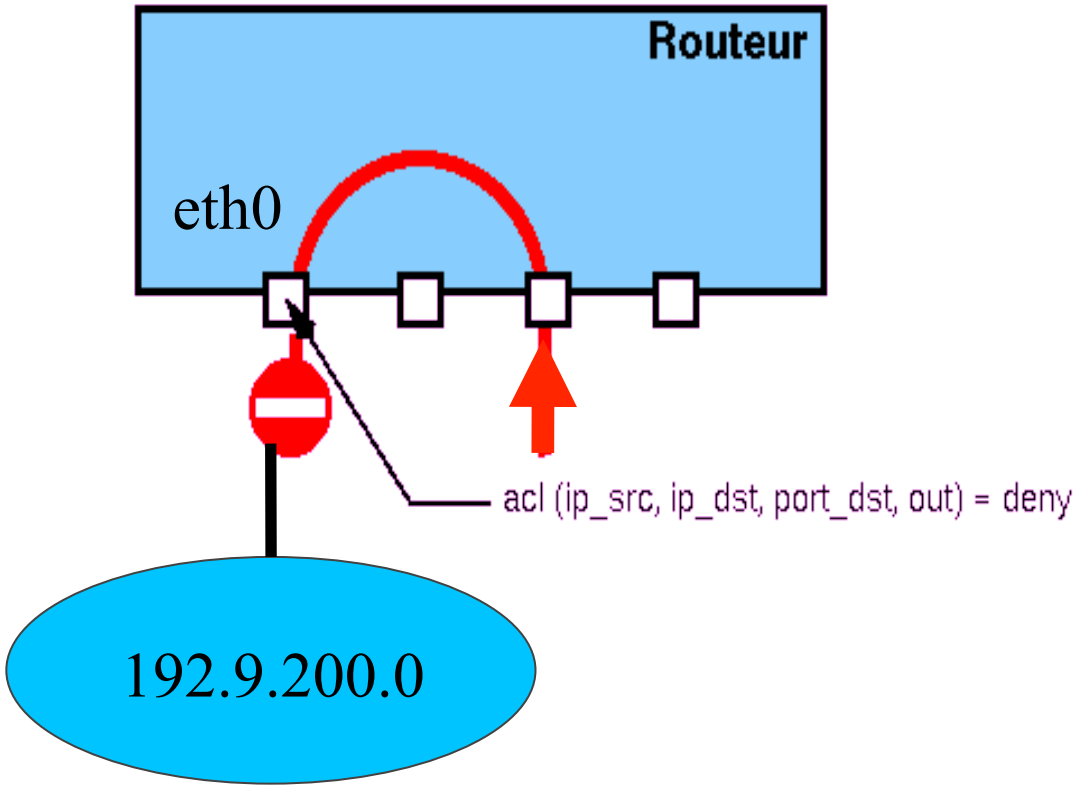
Routeur CISCO : fonctionnement

- Pour chaque paquet IP
  - Vérifier les ACL de l'interface d'entré du paquet
    - Si l'ACL renvoie "deny", alors le paquet est rejeté
  - Vérifier les ACL de l'interface de sortie
    - Si l'ACL renvoie "deny", alors le paquet est rejeté



Routeur CISCO : exemples

- Ne pas Accepter des paquets sur l'interface du réseau externe avec une IP source appartenant au réseau interne ou loopback
  - access-list 101 deny ip 192.9.200.0 0.0.0.255 any log
  - access-list 101 deny ip 127.0.0.0 0.255.255.255 any log



Routeur CISCO : exemples

- Interdiction de ICMP (ping) sur l'adresse broadcast
  - access-list 101 deny icmp any host 192.9.200.255 log
  - access-list 101 deny icmp any host 192.9.200.0 log
- ICMP sur toutes mes machines
  - access-list 101 permit icmp any 192.9.200.0 0.0.0.255

Routeur CISCO : exemples

- Autorise le port 113 (RFC 931, auth) sur mon serveur
  - access-list 101 permit tcp any host 192.9.200.1 eq 113
- Accès aux serveurs de noms primaires et secondaires (DNS)
  - access-list 101 permit udp any host 192.9.200.1 eq domain
  - access-list 101 permit udp any host 192.9.200.2 eq domain
  - access-list 101 permit tcp any host 192.9.200.1 eq domain
  - access-list 101 permit tcp any host 192.9.200.2 eq domain

Routeur CISCO : exemples

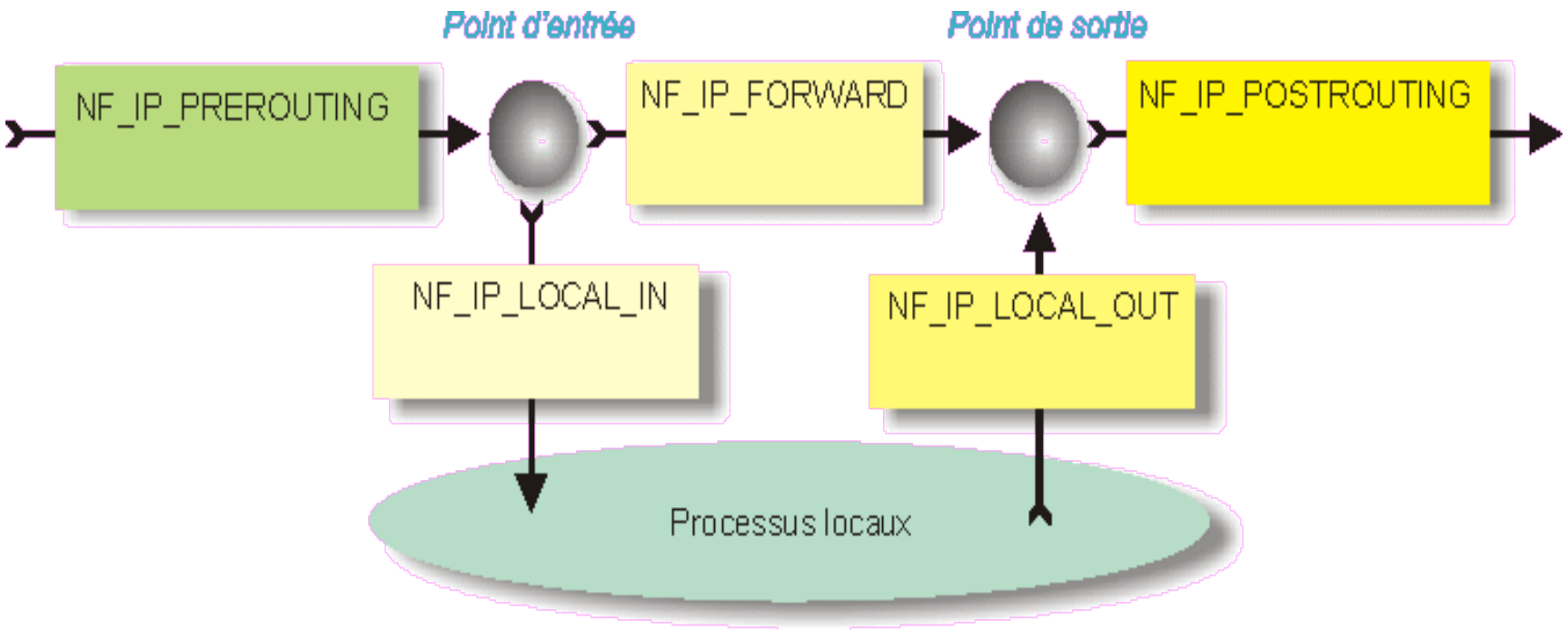
- Accès aux services usuels : mail, ftp, WWW
  - access-list 101 permit tcp any host 192.9.200.1 eq ftp
  - access-list 101 permit tcp any host 192.9.200.1 eq ftp-data
  - access-list 101 permit tcp any host 192.9.200.1 eq smtp
  - access-list 101 permit tcp any host 192.9.200.1 eq www
- Autorise tous les ports TCP superieurs a 1024 (problème FTP)
  - access-list 101 permit tcp any 192.9.200.0 0.0.0.255 gt 1023
- Autorise tous les ports UDP superieurs a 1024 sauf 2049 (NFS)
  - access-list 101 deny udp any 192.9.200.0 0.0.0.255 eq 2049 log
  - access-list 101 permit udp any 192.9.200.0 0.0.0.255 gt 1023

FILTRAGE NETFILTER

Linux : netfilter & iptable

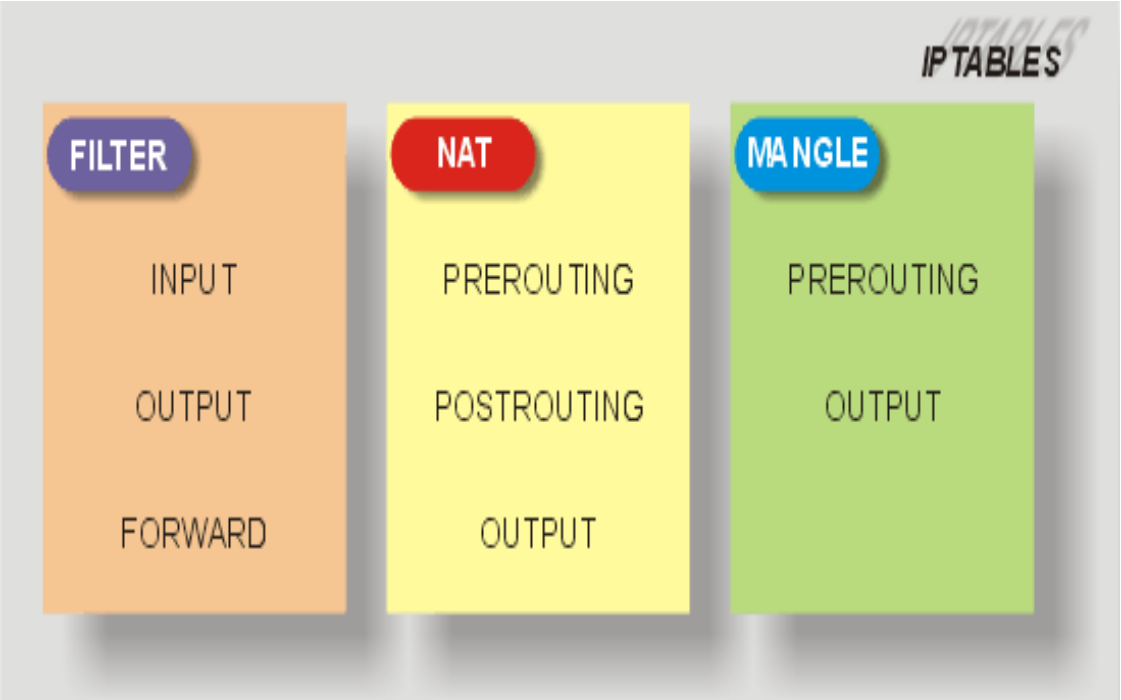
Linux : netfilter & iptable

- Netfilter va être capable :
  - D'effectuer des filtrages de paquets
  - D'effectuer des opérations de NAT (Network Address Translation)
  - D'effectuer des opérations de marquage des paquets



Linux : netfilter & iptable

- Netfilter
  - une commande à tout faire → IPtables
    - Permettre d'écrire des chaînes de règles dans des tables
    - 3 tables correspondant aux 3 principales fonctions



Netfilter & iptable : table filter

- Toutes les règles permettrant de filtrer les paquets
- 3 chaînes
  - La chaîne INPUT
    - Paquets entrant localement sur l'hôte
  - La chaîne OUTPUT
    - Paquets émis par l'hôte local qui seront filtrés
  - La chaîne FORWARD
    - Paquets traversant l'hôte suivant les routes implantées
- Les chaînes
  - ensembles de règles
  - permettre d'identifier des paquets correspondant à certains critères

Netfilter & iptable : les cibles

- Sortes d'aiguillage dirigeant les paquets satisfaisant aux critères
- Les cibles préconstruites sont :
  - ACCEPT
    - Paquets qui satisfont aux critères sont acceptés
    - ils continuent leur chemin dans la pile
  - DROP
    - Paquets qui satisfont aux critères sont rejetés
  - LOG
    - permettre de tracer au moyen de syslog les paquets qui satisfont aux critères.
- Suivant les contextes, d'autres cibles deviennent accessibles
  - REJECT similaire à DROP, mais avec envoi d'un message d'erreur ICMP à la source du paquet rejeté

Netfilter & iptable : suivi de connexion

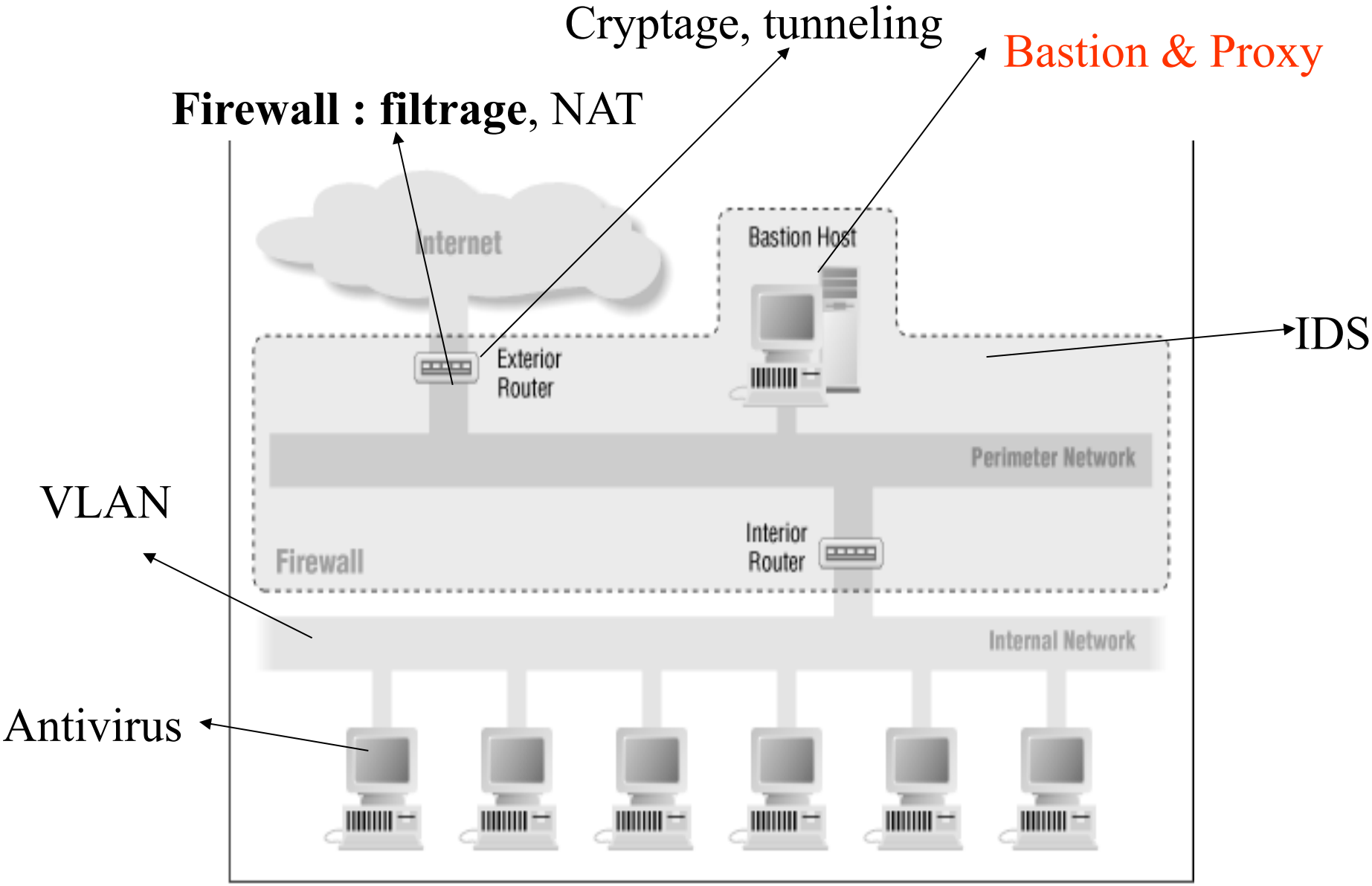
- Suivi de connexion permet de réaliser un "firewall statefull"
  - Mémoriser ce qu'il se passe sur la couche TCP
  - Possiblité de savoir si une connexion est dans l'un de ces états :
    - NEW : nouvelle connexion (elle contient le flag SYN)
    - ESTABLISHED : connexion déjà établie, elle ne devrait pas contenir de SYN ni de FIN
    - RELATED : la connexion présente une relation directe avec une connexion déjà établie,
    - INVALID : la connexion n'est pas conforme, contient un jeu de flags anormal, n'est pas classable dans l'une des trois catégories précédentes.

Netfilter & iptable : UDP

- Problème : pas de connexion
- impossible de définir l'état d'un échange UDP
- Solution : mettre en place un "timer" pour décider de l'état d'un paquet UDP
- Exemple : requête DNS depuis le réseau privé
  - Le premier paquet UDP sort du réseau, sur le port DNS 53
    - →le laisser passer
  - Qualifier de "NEW". déclenche un timer
  - Si avant expiration du timer
    - recevons un paquet UDP dudit serveur DNS
  - considérer que c'est un paquet "ESTABLISHED".

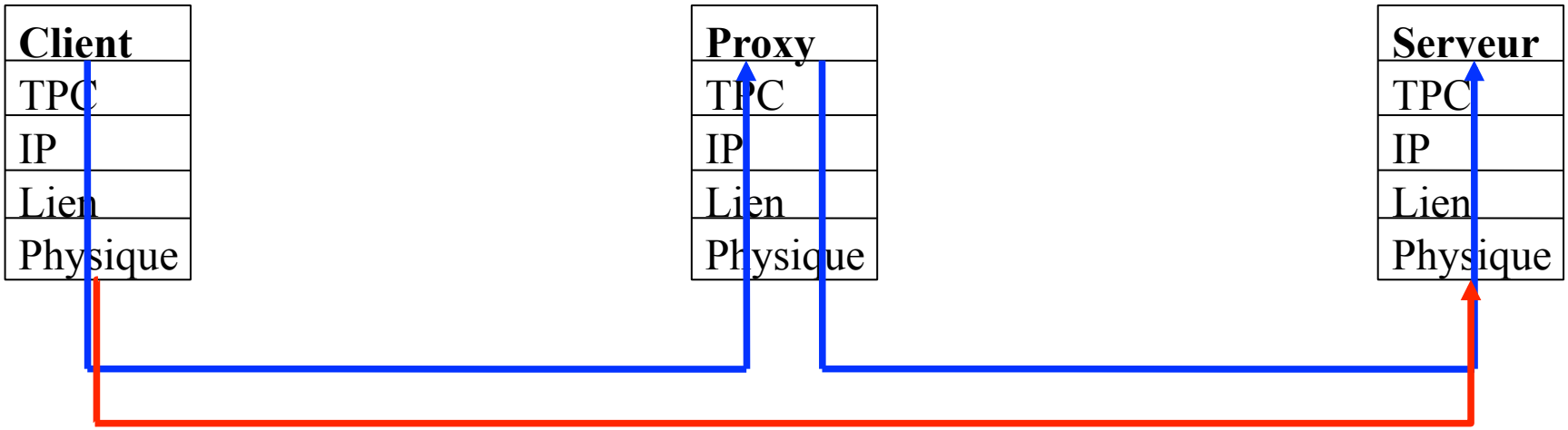
BASTION

Bastion


Cryptage, tunneling
Bastion & Proxy
Firewall : filtrage, NAT
Internet
Bastion Host
IDS
Exterior
Router
Perimeter Network
VLAN
Interior
Router
Firewall
Internal Network
Antivirus

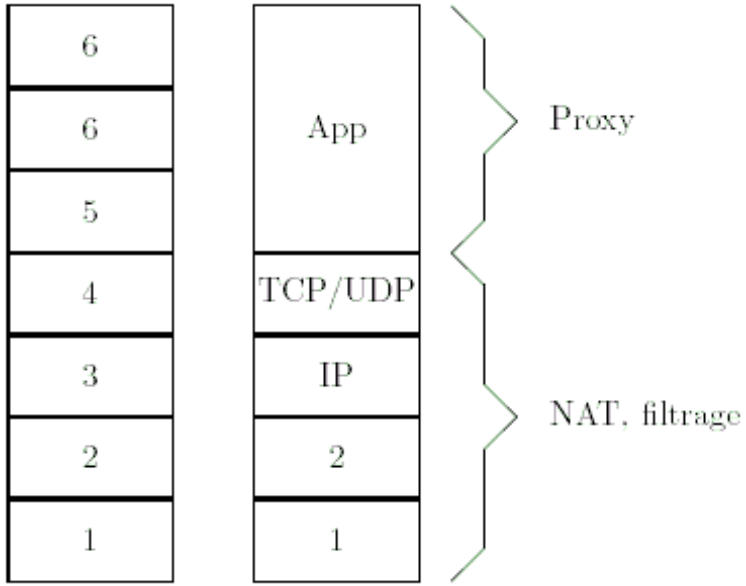
Introduction

- Bastion = 1 machine de la DMZ
  - services accessibles de l'extérieur :
    - Web, FTP, mail, DNS...
- Proxy = Relais d'applications
  - jouent le rôle de serveur pour le client, et de client pour le serveur
  - éviter les connexions directes



Introduction

- Les proxys
  - agissent dans la couche application
  - analyser les données dans le contexte de l'application et filtrer si nécessaire
    - contenu, virus, exploits
- != firewall
  - Les filtres (même à mémoire)
  - NAT
  - couches 1 à 4
- Ici accès aux données
  - couches 5 à 7



Proxy HTTP

- protocole simple après connexion au serveur
  - get /toto/tutu/index.html
- Pour fonctionner avec un proxy, le protocole doit être modifié:
  - le navigateur doit être configuré
    - 1. Adresser toutes ces requêtes à l'adresse et au port prédéfini du proxy
    - 2. Indiquer l'URL complète dans ces requêtes
      - plutôt que le chemin relatif du document
  - La même requête serait donc :
    - get http://www.toto.com/toto/tutu/index.html

Proxy HTTP

- Cache
  - Garder une copie locale de tous les documents
  - Quand un deuxième client demande le même document → fournir la copie locale
  - Avantage
    - Transfert est beaucoup plus rapide (augmentation du confort)
    - Economiser de la bande passante (limitation des coûts)

Proxy HTTP

- Avant de fournir une copie d'un document
  - s'assurer que l'original n'a pas changé
  - ajouter le paramètre "if modified since:" à sa requête.
    - Si le document n'a pas changé, le serveur répond "not modified",
    - sinon il fournit le document
  - Si le document à une date de péremption
    - pas besoin d'interroger le serveur

Proxy HTTP

- filtrage de contenu
  - Anti-virus
    - Examiner le contenu de tous les documents téléchargés
    - Protection contre
      - certains vers (comme nimda)
      - messagerie par le web : les attachements sont transmis par le protocole HTTP
  - Filtrage parental
    - Interdire l'accès à certains sites web
      - Catégorisation automatique des sites
        - taux de FA / FR
      - besoin de MAJ

SMTP

- Protocole a été conçu pour les relais
  - Serveurs SMTP agissent comme proxy
- Fonctionnement
  - serveur SMTP utilisent la base de donnée DNS pour connaître le serveur destinataire
    - DNS contient des entrées du type MX
    - indiquant quels sont les serveurs SMTP responsables d'un domaine
  - transférer le message à l'aide d'une connexion SMTP

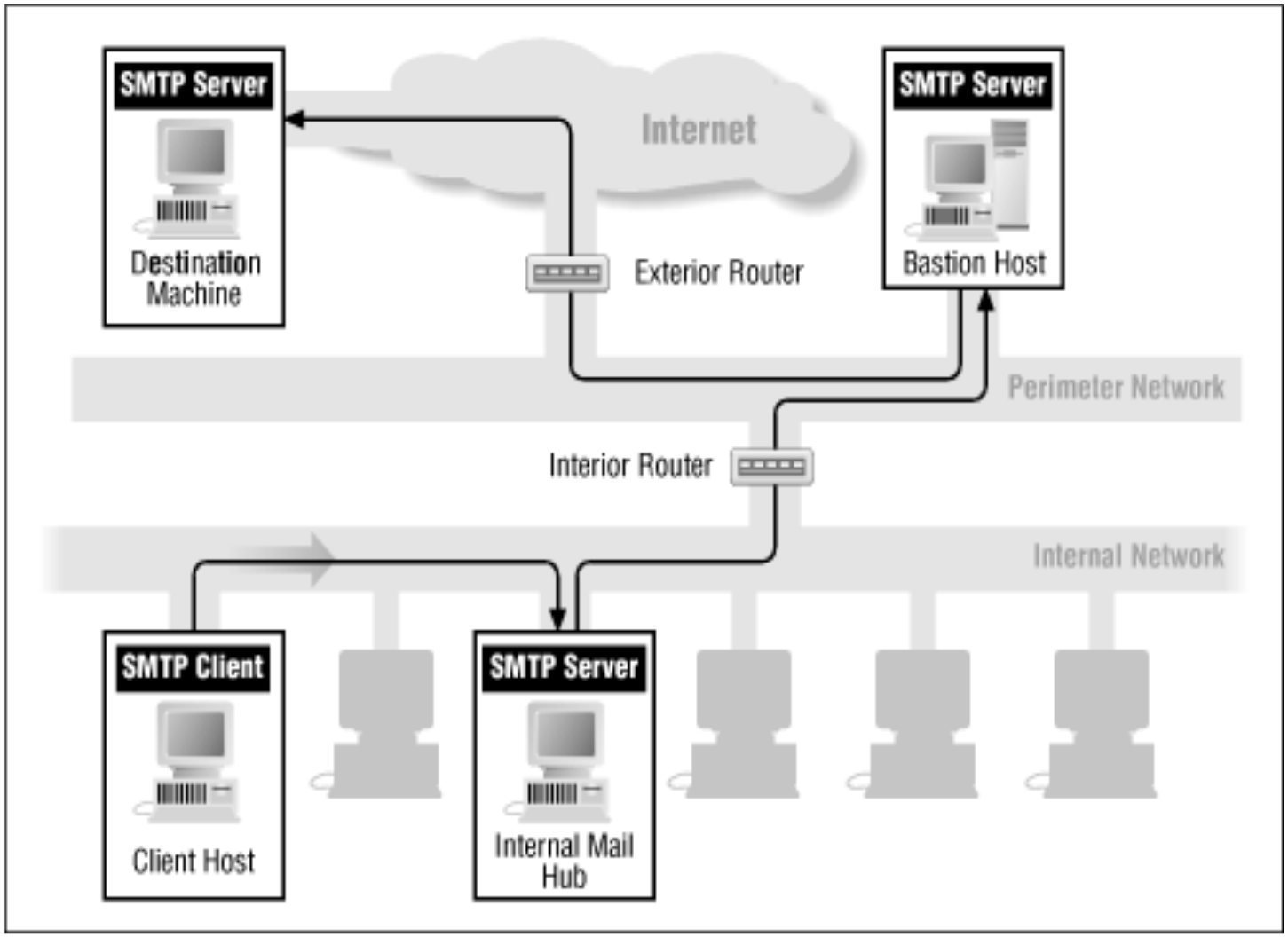
SMTP

- Configuration
  - 1. Pour le mail sortant:
    - Configurer les serveurs ou clients internes
      - utiliser le proxy comme destination pour leurs connexions SMTP
      - et non les serveurs indiqués dans les MX-records.
  - 2. Pour le mail entrant:
    - Inscrire dans le DNS le serveur proxy comme responsable du domaine
    - indiquer au proxy ou se trouve le serveur interne qui doit normalement recevoir le courrier entrant.

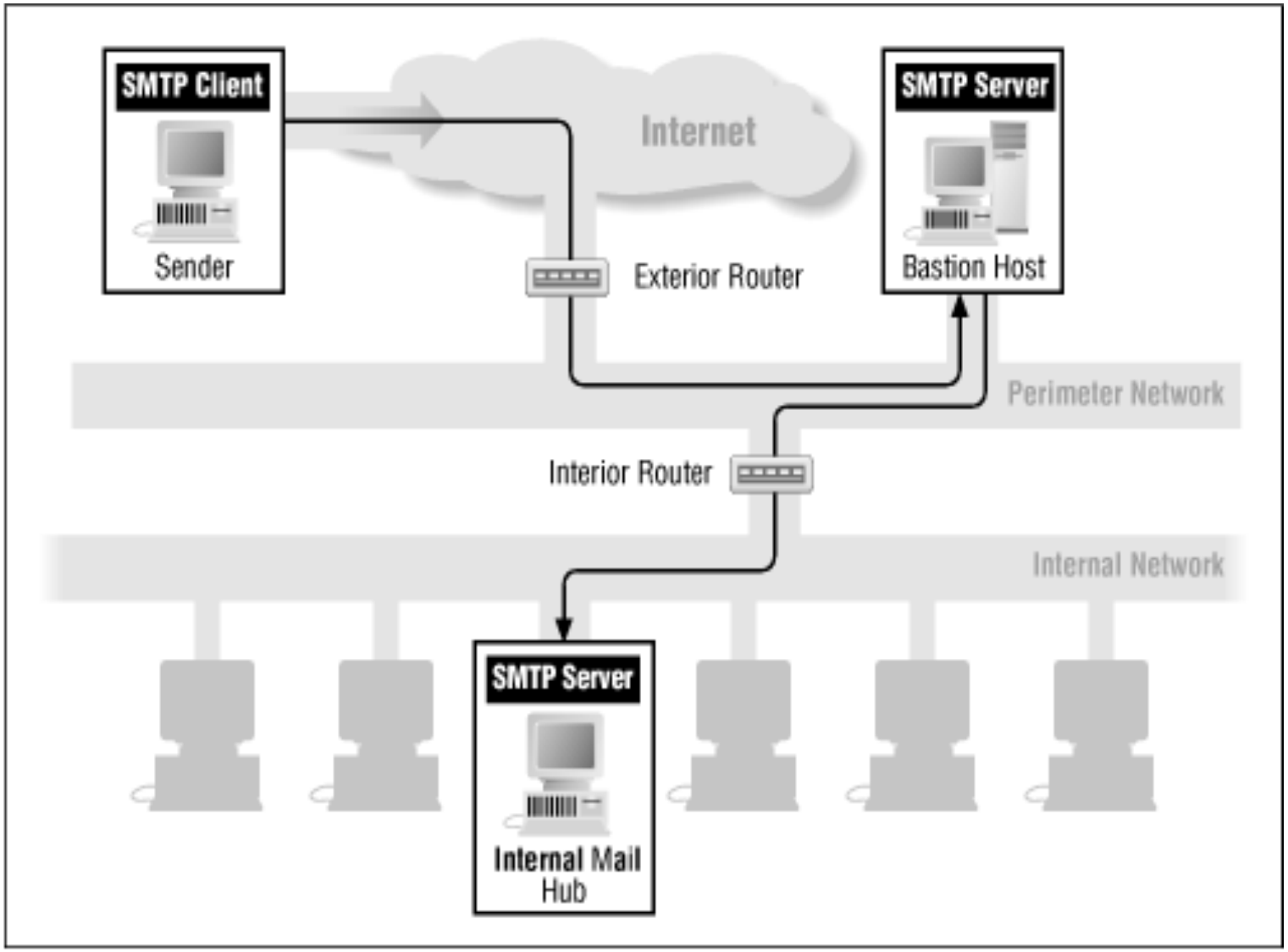
SMTP

- Attention
  - Relais de mail --> lutter contre le spam
  - pour éviter que le proxy soit abusé
    - L'expéditeur ou le destinataire des messages relayés doit être local
    - Seules les machines locales ont le droit de spécifier des expéditeurs locaux

SMTP


SMTP Server
Destination Machine
Internet
Exterior Router
SMTP Server
Bastion Host
Perimeter Network
Interior Router
Internal Network
SMTP Client
Client Host
SMTP Server
Internal Mail Hub

SMTP


SMTP Client
Sender
Internet
SMTP Server
Bastion Host
Exterior Router
Perimeter Network
Interior Router
Internal Network
SMTP Server
Internal Mail
Hub

Proxy HTTPS

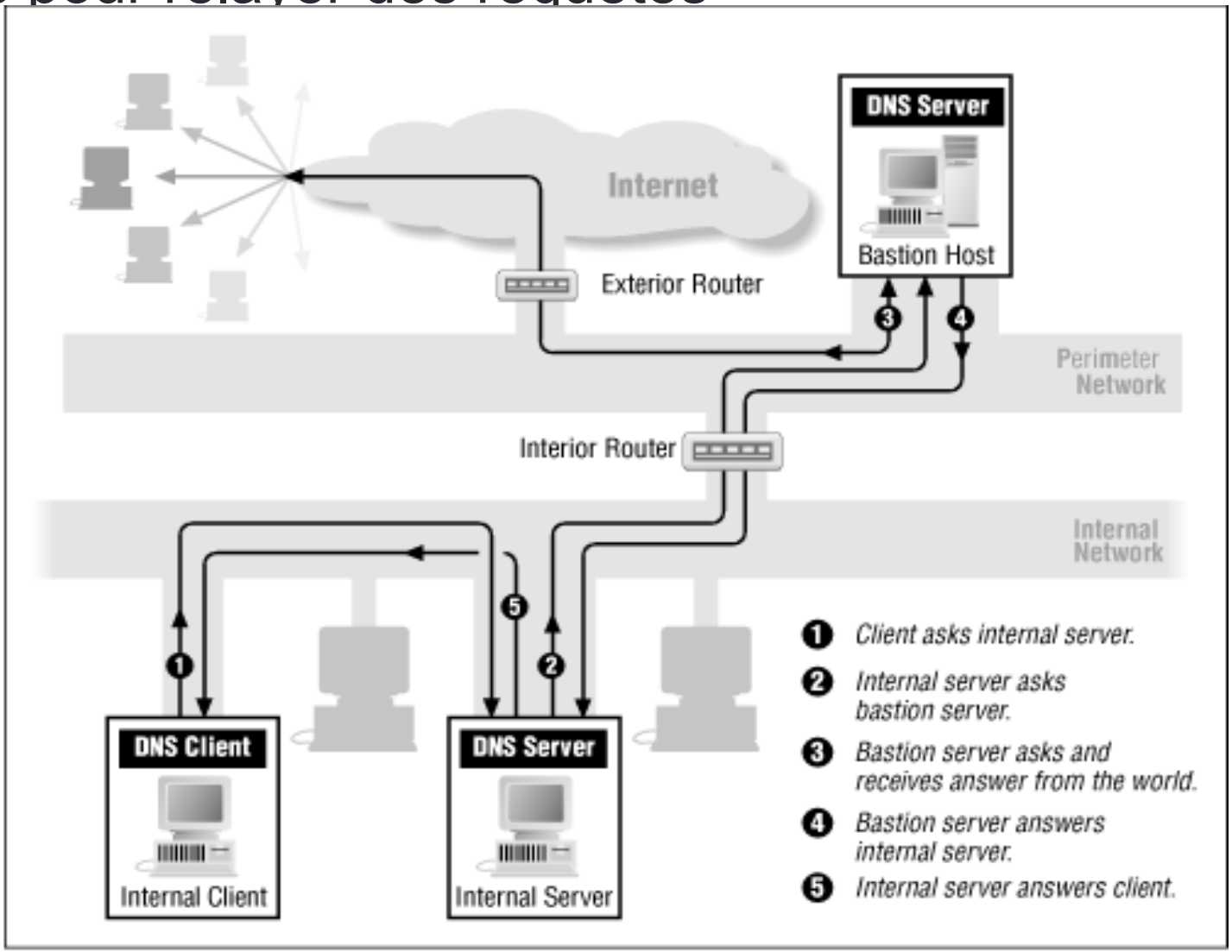
- HTTPS est la version sécurisée de HTTP
  - Les proxy HTTPS ne sont PAS une version sécurisée des proxys HTTP !
- HTTPS chiffre et authentifie de bout en bout
  - Si c'est le proxy qui fait la connexion, on perd tous les avantages.
  - Le proxy HTTPS se contente donc de relayer de manière transparente les données entre une connexion client et une connexion serveur

Proxy HTTPS

- Proxy HTTPS permet de relayer n'importe quel protocole
  - il est transparent
  - limiter les abus, utiliser des ports spécifiques 443 (HTTPS) et 563 (SNEWS)
  - Pour traverser un firewall, il suffit de faire tourner le serveur sur le port 443 et passer par un proxy HTTPS !!!

DNS

- Conçus pour relayer des requêtes



Les Proxys inverses

- En sens direct
  - le client sait qu'il doit passer par un proxy, il peut adapter ses requêtes en conséquence
- En sens inverse
  - le client ne sait pas s'il parle à un serveur ou à un proxy
  - Le proxy doit agir de manière identique à un serveur

Les Proxys inverses

- Les proxy inverses HTTP permettent :
  - De filtrer les requêtes (blocage des exploits)
  - D'authentifier les clients avant même qu'ils ne parlent au serveur
  - D'accélérer les serveurs : fonctionnent comme cache, load balancing
    - le proxy fournit les documents statiques
    - le serveur n'a plus qu'à générer les documents dynamiques (e-commerce)