Cours de sécurité

Pare-feux ('Firewalls')

Gérard Florin
- CNAM -
- Laboratoire CEDRIC -

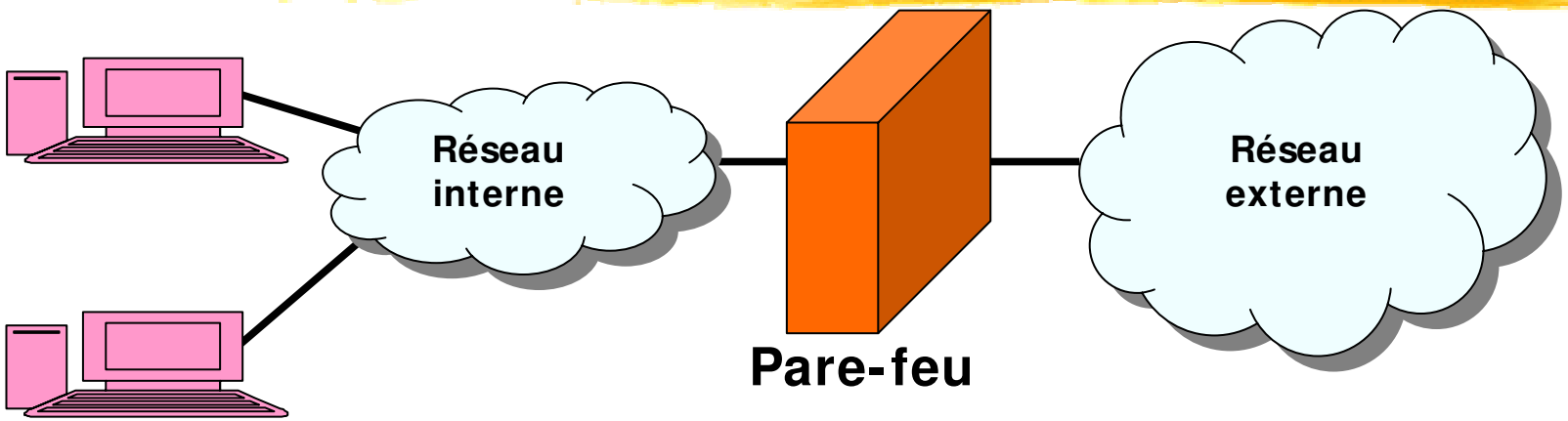
Plan pare-feux

- Introduction
- Filtrage des paquets et des segments
- Conclusion
- Bibliographie

Pare-Feux

Introduction

Pare-feux ('firewalls'): Architecture de base



- **1) Un domaine à protéger : un réseau 'interne'.**
  - Un réseau d'entreprise/personnel que l'on veut protèger
  - Vis à vis d'un réseau 'externe' d'ou des intrus sont suceptibles de conduire des attaques.
- **2) Un pare-feu**
  - Installé en un point de passage obligatoire entre le réseau à protéger (interne) et un réseau non sécuritaire (externe).
  - C'est un ensemble de différents composants matériels et logiciels qui contrôlent le traffic intérieur/extérieur selon une politique de sécurité.
  - Le pare-feu comporte assez souvent un seul logiciel, mais on peut avoir aussi un ensemble complexe comportant plusieurs filtres, plusieurs passerelles, plusieurs sous réseaux ….

Pare-feux ('firewalls'): Définitions de base

- **1) 'Firewall' :** en anglais un mur qui empêche la propagation d'un incendie dans un bâtiment => Français '**mur pare-feu'.**
- **2) Pare-feu :** en informatique une protection d'un réseau contre des attaques.
- **3) Technique employée** : le contrôle d'accès (le filtrage).
  - **a) Notion de guichet** : restriction de passage en un point précis et contrôle des requêtes.
  - **b) Notion d'éloignement** : empêcher un attaquant d'entrer dans un réseau protégé ou même de s'approcher de trop prés de machines sensibles.
  - **c) Notion de confinement** : empêcher les utilisateurs internes de sortir du domaine protègé sauf par un point précis.
  - **d) Généralement** un pare-feu concerne les couches basses Internet (IP/TCP/UDP), mais aussi la couche application (HTTP, FTP, SMTP….).
- **4) Image militaire** la plus voisine de la réalité d'un pare-feu: les défenses d'un chateau-fort (murailles, douves, portes/pont levis, bastion=> confinement, défense en profondeur, filtrage).

Pare-feux : le possible et l'impossible

Ce que peut faire un pare-feux :

- 1) Etre un guichet de sécurité: un point central de contrôle de sécurité plutôt que de multiples contrôles dans différents logiciels clients ou serveurs.
- 2) Appliquer une politique de contrôle d'accès.
- 3) Enregistrer le traffic: construire des journaux de sécurité.
- 4) Appliquer une défense en profondeur (multiples pare-feux)

Ce que ne peut pas faire un pare-feux :

- 1) Protèger contre les utilisateurs internes (selon leurs droits).
- 2) Protèger un réseau d'un traffic qui ne passe pas par le pare-feu (exemple de modems additionnels)
- 3) Protéger contre les virus.
- 4) Protéger contre des menaces imprévues (hors politique).
- 5) Etre gratuit et se configurer tout seul.

Définir un politique de sécurité 1) Interdire tout par défaut

- **Présentation générale de cette approche:**
  - Tout ce qui n'est pas explicitement permis est interdit.
- **Mise en oeuvre** :
  - **Analyse** des services utilisés par les utilisateurs.
    - **Exemple 1 :** Un hôte serveur de courrier doit pouvoir utiliser SMTP.
    - **Exemple 2 :** Un hôte devant accèder au Web doit pouvoir utiliser HTTP.
  - **Définition des droits à donner :** définition de la politique de sécurité.
  - **Attribution des droits** dans un outil appliquant la politique, **Suppression de tous les autres droits.**
- **Avantages/ inconvénients**
  - **Solution la plus sécuritaire et la plus confortable pour l'administrateur de la sécurité.**
  - **Solution qui limite considérablement les droits des usagers.**
- **Solution la plus recommandée et la plus souvent utilisée.**

Politiques de sécurité : 2) Autoriser tout par défaut

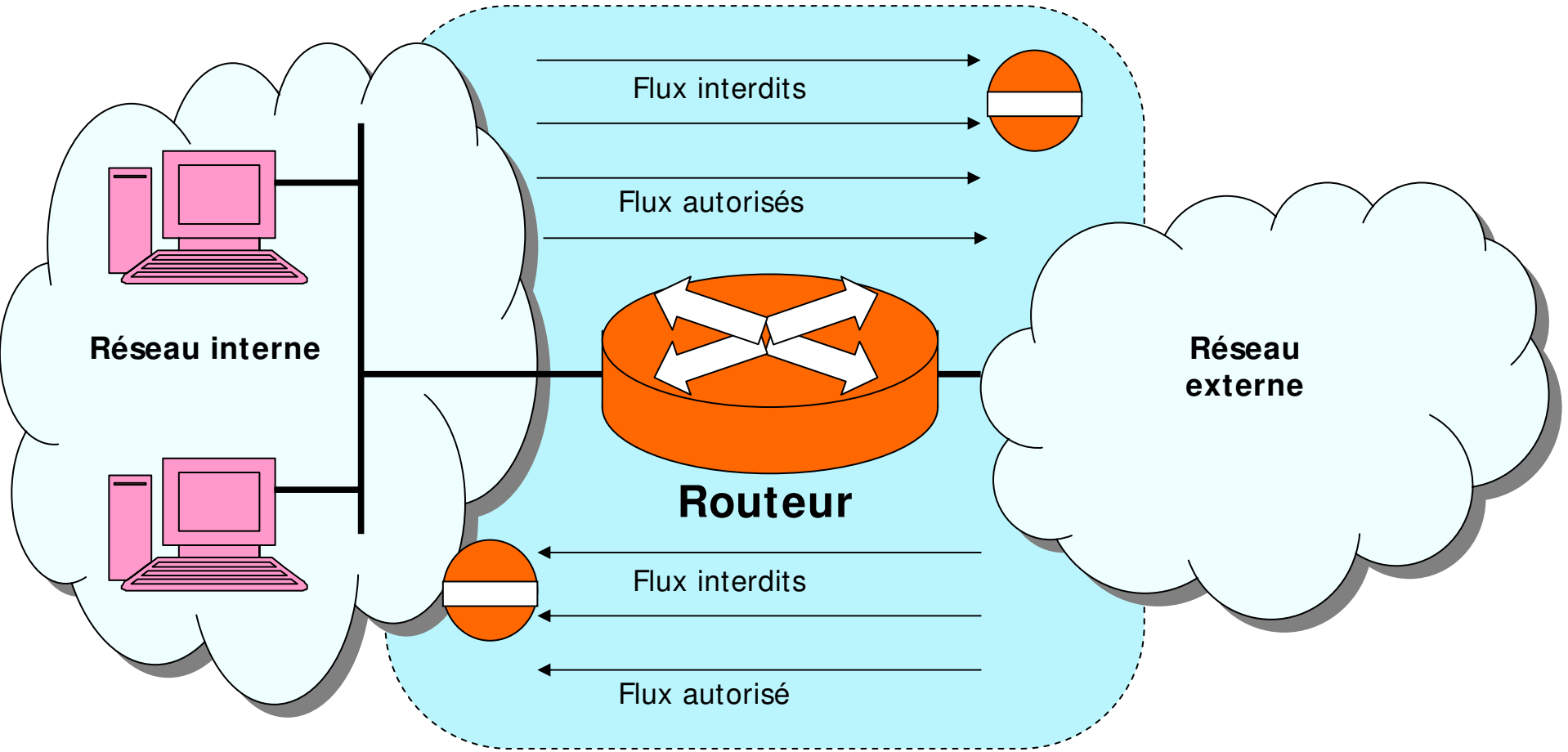
- **Présentation générale de la solution :**
  - On permet tout sauf ce qui est considéré comme dangereux => Tout ce qui n'est pas explicitement interdit est autorisé.
- **Mise en oeuvre :**
  - On analyse les différents risques des applications qui doivent s'exécuter.

  => On en déduit les interdictions à appliquer, on autorise tout le reste.
  - **Exemple 1 :** Interdire complètement les accès en Telnet depuis l'extérieur ou les autoriser sur une seule machine.
  - **Exemple 2 :** Interdire les transferts FTP ou les partages NFS depuis l'intérieur (protection des données).
- **Avantages/ inconvénients**
  - **Solution inconfortable pour l'administrateur de la sécurité.**
  - **Solution qui facilite l'accès des usagers au réseau.**
- **Solution peu recommandée et peu utilisée.**

Outils dans les pare-feux : 1) Filtre de paquets et de segments

- **Concerne le trafic échangé** aux niveaux IP (paquets) et TCP/UDP (segments).
- **Ensemble de règles autorisant ou refusant un transfert combinant la plupart des informations disponibles** dans les messages : adresses sources destination, indicateurs ….
- **En fait** : définition d'une politique de sécurité à capacités.
- **Solution implantée à de nombreux emplacements dans les réseaux:** ordinateurs clients ou serveurs, routeurs filtrants ('screening router'), équipements dédiés.
- **Avantages :** solution peu coûteuse et simple agissant sur tous les types de communications.
- **Inconvénients :**
  - Des règles de filtrage correctes et bien adaptées aux besoins peuvent être difficiles à établir.
  - On n'agit qu'aux niveaux 3 et 4.

Architecture de pare-feu avec routeur filtrant ('screening router')



Outils dans les pare-feux : 2) Filtre applicatif ('proxy')

- **Proxy de sécurité :** analyse du trafic échangé au niveau application (niveau 7) pour appliquer une politique de sécurité spécifique de chaque application.
- **Un serveur proxy est nécessaire** : pour chaque protocole d'application SMTP, FTP, HTTP, ...
  - parcequ'il faut interprèter les messages de façon différente pour chaque application.
- **Contrôle des droits :** implique que chaque usager soit authentifié.
- **Avantage :** on peut intervenir de manière fine sur chaque zone des charges utiles transportées au niveau applicatif.
- **Inconvénient :** solution coûteuse car il faut définir des droits complexes.

Outils dans les pare-feux : 3) Hôte à double réseau

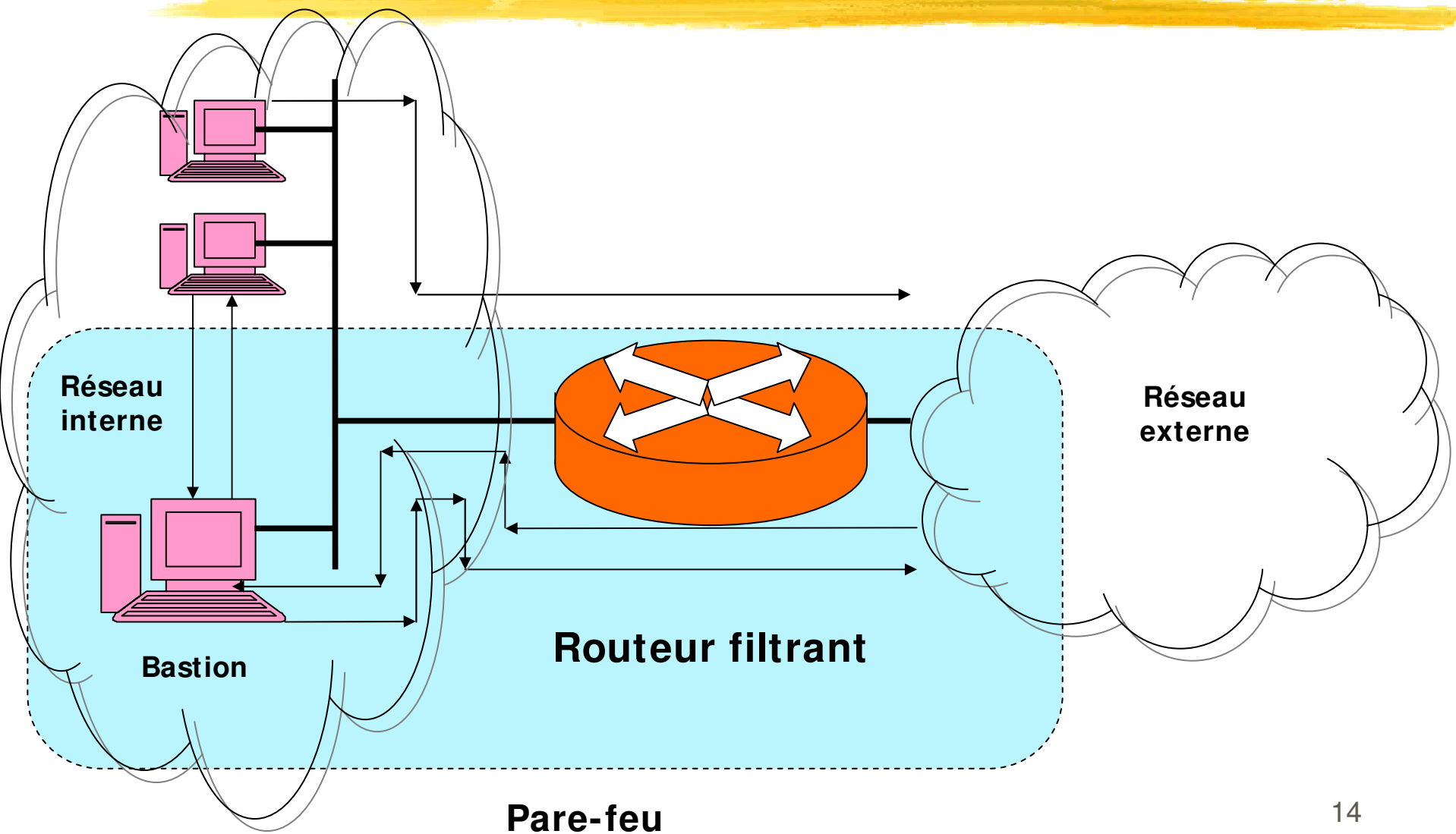
- **Terminologie :** Hôte à double réseau

  En anglais ‘Dual homed host’.
- **Définition :**
  - Un hôte qui possède au moins deux interfaces réseaux (qui interconnecte au moins deux réseaux).
- **Propriété:**
  - Si un hôte connecte deux sous réseaux,
  - Et s’il n’est pas configuré en routeur.
  - => Il est impossible à un paquet de passer d’un réseau à l’autre sans être traité au niveau applicatif.
  - => C’est un proxy incontournable.

Outils dans les pare-feux : 4) Bastion

- **Définition :**
  - Un hôte exposé au réseau externe (rendu accessible de l'extérieur par la définition de la politique de sécurité).
  - Il constitue un point de contact entre réseau externe et réseau interne.
- **Serveur pour un ensemble de services prédéfinis** :
  - Service toile (HTTP), service de noms (DNS), service de messagerie ….
  - Le bastion peut agir en rendant directement le service concerné.
  - Le bastion peut agir en relayant les requêtes vers d'autres serveurs après avoir effectué un contôle d'accès applicatif (proxy-serveur).
  - Le bastion doit être incontournable pour l'ensemble des services prévus.
- **Le bastion peut servir dans la détection d'intrusion:**
  - **Analyse des communications** pour détecter des attaques : IDS ('Intrusion Detection System').
  - **Fonction pot de miel (Honeypot)** : un service semblant attractif pour un attaquant et qui n'est en réalité qu'un piège pour détecter l'attaquant.

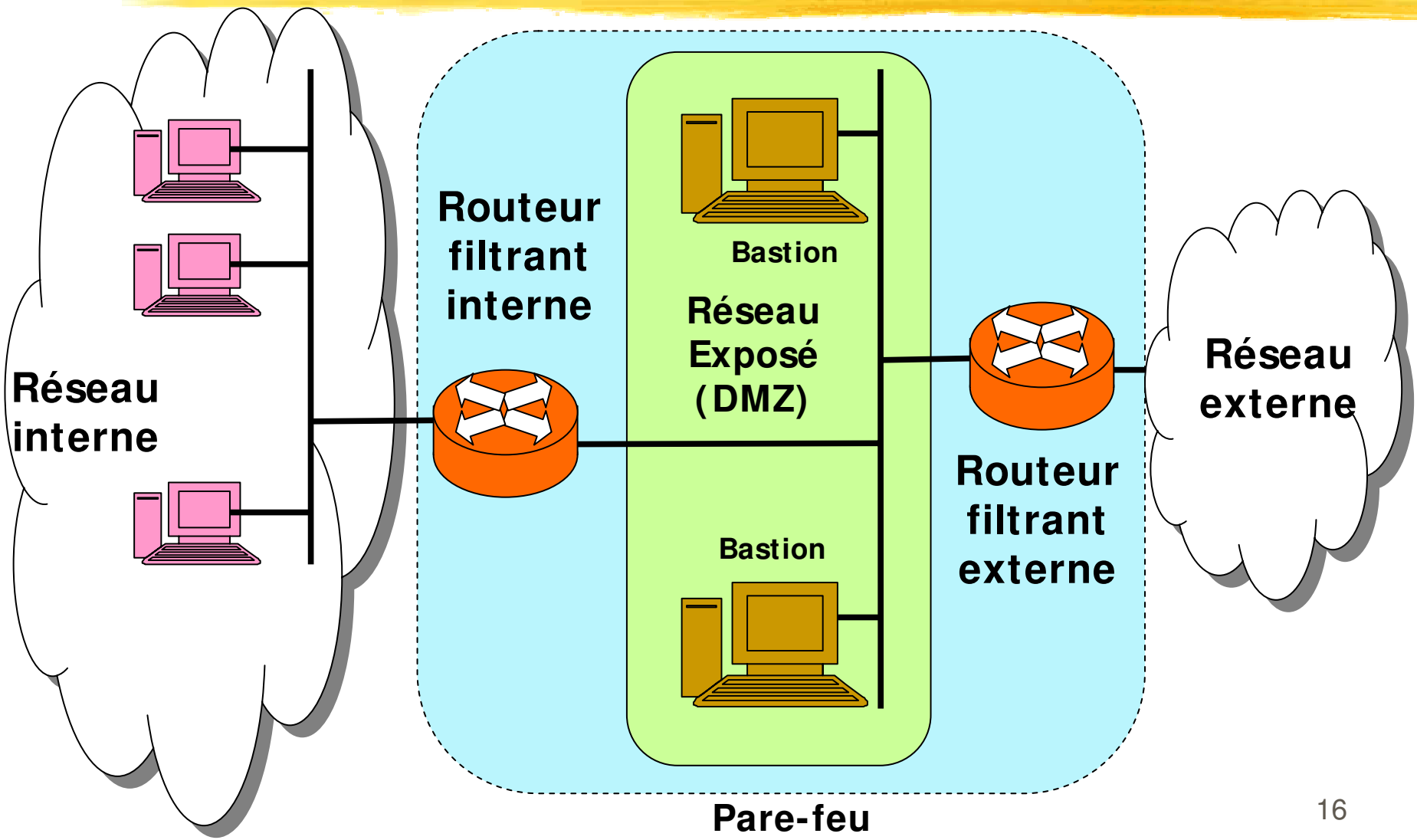
Architecture de pare-feu avec routeur filtrant et bastion



Outils dans les pare-feux : 5) Zone démilitarisée (réseau exposé)

- **Terminologie :**
  - Réseau exposé, réseau périphérique ('Peripheral Network')
  - Zone démilitarizée , DMZ, 'De Militarized Zone'
- **Définition :**
  - Une partie d'un pare-feu qui est un sous-réseau.
  - Ce sous réseau placé en passerelle entre un réseau à protéger et un réseau externe non protégé.
- **Propriétés visées :**
  - La zone démilitarizée est plus ouverte sur le réseau externe que le réseau interne.
  - Elle dessert les systèmes exposés à l'extérieur : principalement les bastions .

Architecture de pare-feu avec routeurs, bastions et DMZ



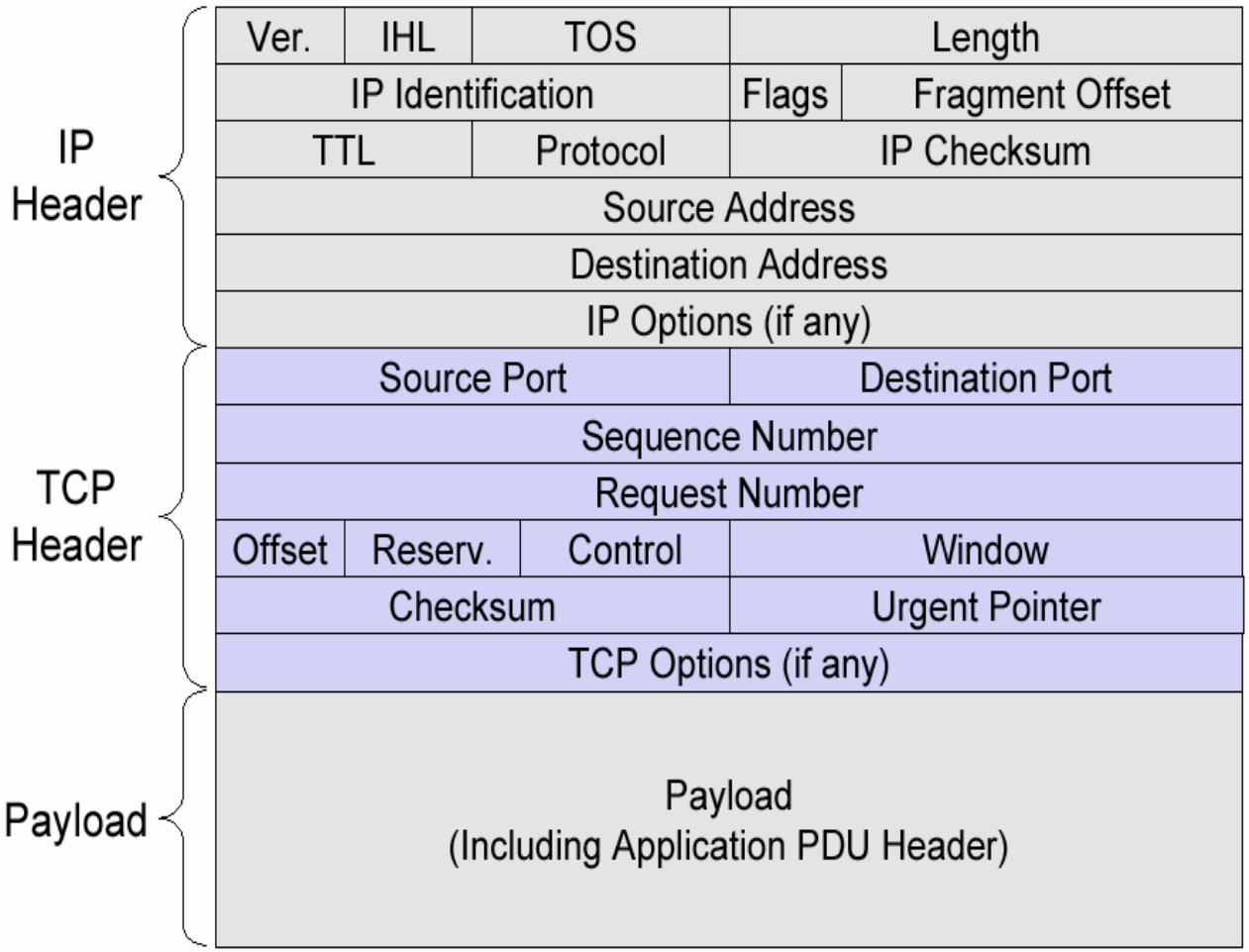
En association avec le pare-feu : 6) Traducteur d'adresses NAT

- **Traduction des adresses IP et TCP** :
  - **NAT** 'Network Address Translation' et **PAT** 'Port Address Translation' => **Traduction combinée** de port et d'adresse réseau: **NAPT** 'Network Address and Port Translation'.
  - Solution introduite pour économiser des adresses IP V4.
- **Solution utilisée en sécurité**:
  - **NAPT permet de cacher le plan d'adressage interne:** les adresses IP et les numéros de port ne sont plus connus à l'extérieur.
  - **NAPT n'autorise pas les connexions initialisées** depuis le réseau externe.
  - Solution différente du filtrage de paquets mais solution complémentaire.

Pare-Feux

Filtrage des paquets et des segments

Rappel: Structure d'un datagramme IP avec un segment TCP



Zones importantes pour les pare-feux (1)

- **Protocole de niveau liaison (PPP, niveau mac):**
  - Zone protocole utilisateur (démultiplexage): IP, IPX ...
  - Zones adresses: Adresses Ethernet IEEE802, (permettent de déterminer la source et la destination sur la liaison donc l'entrée ou la sortie)
- **Protocole IP:**
  - Adresses source et destination.
  - Drapeaux (Flags): en particulier ceux qui concernent la fragmentation.
  - Le type de protocole destinataire: TCP, UDP, ICMP, ...
  - Analyse des zones d'extension par exemple en routage par la source => Demande de destruction de ces datagrammes car utilisation possible du routage par la source en attaque.

Zones importantes pour les pare-feux (2)

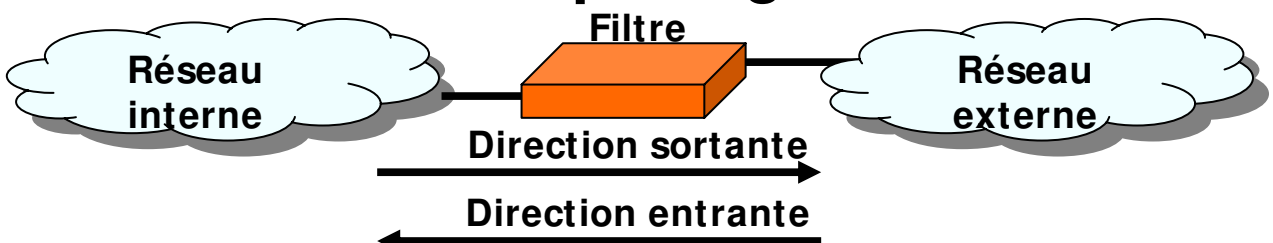
- **Protocole TCP :**
  - **Numéros de port source et destination:** permet d'estimer quel est le service concerné dans la mesure ou l'on respecte l'utilisation des numéros bien connus => Il est toujours possible pour un attaquant d'usurper un numéro de port.
  - **Drapeaux de contrôle (flags)**
  - **ACK:** positionné sauf dans le premier segment (utilisation possible pour bloquer des connexions).
  - **SYN:** positionné dans les deux premiers segments (permet d'identifier les connexions).
  - **RST:** fermeture non négociée de connexion.
- **Protocole d'application :**
  - Analyse non réalisée par les filtres de paquets mais par les proxys serveurs.
  - L'application filtrée doit être très stabilisée.

Les principaux services Internet à contrôler

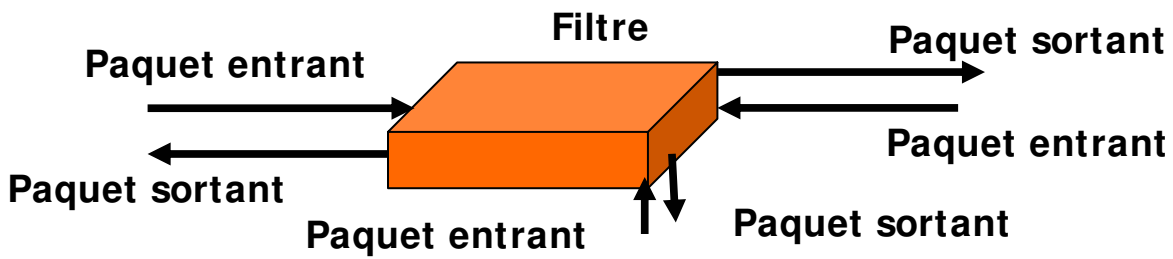
- **Le courrier électronique SMTP** Simple Mail Transfer Protocol.
- **Le transfert de fichiers FTP** File Transfer Protocol et **l'accès fichier distant** NFS Network File System.
- **Les accès à distance** protocoles telnet, rlogin, ssh
- **La toile** HTTP Hypertext Transfer Protocol
- **Les informations sur les utilisateurs:** finger
- **Les services de conferences** CUseeMe, Netmeeting, …
- **L'annuaire des noms de domaine DNS** Domain Name Service.
- **L'administration de réseau SNMP** Simple Network Management Protocol.
- **La synchronisation d'horloges NTP** Network Time Protocol.
- **Les systèmes multi fenêtres X-Windows**
- **Les systèmes d'impressions LPR/ LPD** Line Printing
- **Les nouvelles (news) NNTP** Network News Transfer Protocol.

Sémantique du filtrage des paquets : Trois notions de direction (1)

- **Les règles sont assez souvent exprimées selon une notion de direction : entrant ou sortant.**
- **1) Direction associée au réseau à protéger.**



- **Les règles ne sont pas symétriques** : on donne des droits à un hôte interne vers l'extérieur et on refuse ces droits de l'extérieur vers l'intérieur.
- **2) Position du filtrage dans un routeur filtrant selon l'interface.**



- **Application d'une règle de filtrage :** soit des la réception (on filtre les paquets arrivés) ou avant l'émission (on filtre les paquets après le routage juste avant la sortie)

Sémantique du filtrage des paquets : Trois notions de direction (2)

- **3) Notion de direction selon le sens de connexion**
  - La direction concerne des connexions (ouvreur actif TCP vers ouvreur passif) ou des services applicatifs (client/serveur).
  - **Règles concernant des services sortants :** la connexion est à la demande d'un ouvreur ou d'un client interne (Exemple: telnet sortant).
  - **Règles concernant des services entrants :** la connexion est à la demande d'un ouvreur ou d'un client externe (Exemple: http entrant).

- **Conclusion :** Introduction dans certains filtres d'un sémantique de sens dans l'expression des règles => Bien connaître la sémantique de la direction dans le filtre utilisé concernant les notions d'entrant et de sortant.

Les trois étapes du filtrage : Etape 1 : Spécification abstraite

- **Définir abstraitement la politique de sécurité :** ce qui est autorisé et ce qui est interdit
  - **Choisir une politique d'ensemble:**

    Solution 1) Tout ce qui n'est pas explicitement autorisé est interdit.

    Solution 2) Tout ce qui n'est pas explicitement interdit est autorisé.
  - **Enoncer des règles**

Exemple de règle 1) Autoriser un hôte intrene à recevoir du courrier électronique de toute provenance parceque c'est un serveur de courrier smtp.

Exemple de règle 2) Interdire à un hôte externe précis d'envoyer du courrier SMTP à un serveur de courrier interne parcequ'il est en liste noire.

Les trois étapes du filtrage : Etape 2: Etablir des règles précises

- **Traduire la politique de sécurité en des règles précises concernant des communications IP**
  - Régles concernant des datagrammes IP : adresses source/destination, protocole utilisateur TCP port source/destination, indicateurs TCP, autres
  - Exemple 1) Règle interdisant tout par défaut

Règle	IP Source	Port Source	IP Dest	Port Dest	Complément
Interdire	*	*	*	*	TCP

  - Exemple 2) Règle autorisant la reception du courrier par un serveur

Règle	IP Source	Port Source	IP Dest	Port Dest	Complément
Autoriser	*	*	Smtp-local	25	TCP

  - Exemple 3)Règle interdisant l'émission par un serveur de courrier suspect

Règle	IP Source	Port Source	IP Dest	Port Dest	Complément
Interdire	Smtp_distant	*	*	*	TCP

Les trois étapes du filtrage : Etape 3 : Configurer un outil précis

- **Rentrer les règles dans un pare-feu réel en utilisant la syntaxe et la sémantique de l'interface de l'outil**
  - Sémantique la plus fréquente : exploitation des règles dans l'ordre.
  - La première règle satisfaite provoque l'autorisation de la transmission ou la destruction du datagramme.
  - En fait un pare-feu interprète un programme qui est une suite de: si (condition sur datagramme) alors action (autoriser/interdire).
  - Exemple : Liste ordonnée des règles précédentes.

Règle	IP Source	Port Source	IP Dest	Port Dest	Complément
Interdire	Smtp-distant	*	*	*	TCP
Autoriser	*	*	Smtp_local	25	TCP
Interdire	*	*	*	*	TCP

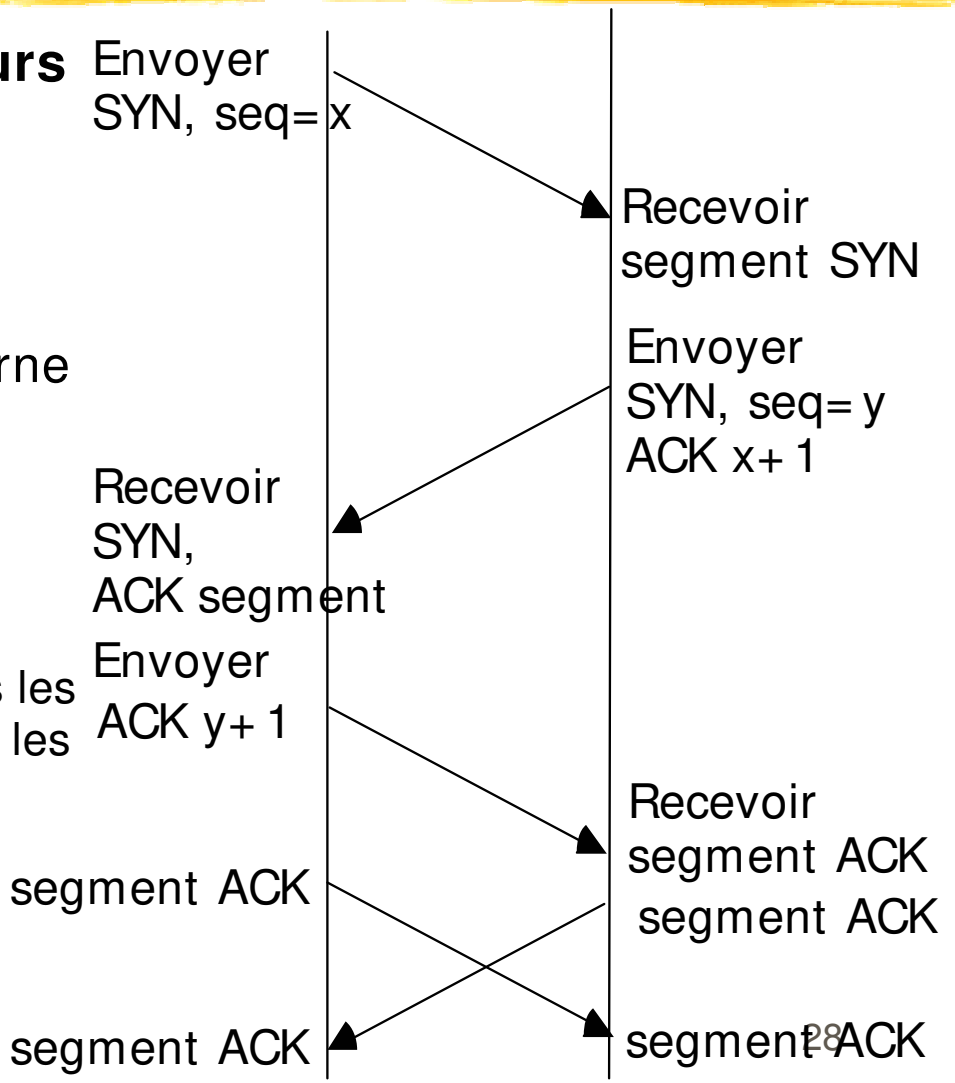
  - Transformer les règles dans la syntaxe du pare-feu disponible

Exemple : Syntaxe de règle avec le pare-feu LINUX (iptables).

[root@ firewall]# iptables –A FORWARD –p smtp –d 192.168.0.10 –j ACCEPT

Affiner les règles de filtrage
Utilisation des indicateurs : ACK

- **Exemple d'utilisation d'indicateurs ('flags') TCP.**
- **Besoin fréquent :** autoriser la connexion d'un client interne sur un serveur interne (ou externe) mais refuser la connexion d'un client externe sur le même serveur interne.
- **Une solution :** l'utilisation de l'indicateur ACK en TCP.
- **Rappel :** Fonctionnement de l'ACK.
  - ACK présent dans pratiquement tous les segments sauf le premier (exception les segments RST qu'on peut autoriser explicitement).
  - Il suffit de bloquer un segment sans ACK pour interdire la mise en place donc l'existence d'une connexion.



Filtrage avec indicateur ACK TCP : Fonctionnement précis

- **Première politique : un client autorisé peut utiliser un service de numéro de port bien connu ou qu'il soit.**
  - La première régle autorise certains hôtes sélectionnés (possiblement tout mon domaine) à communiquer avec un service distant (interne ou externe) de numéro de port bien connu (noté ici service-tcp, par ex 80).
- **Seconde politique : un site externe ne peut commencer une communication avec un serveur interne sur le port bien connu mais il peut continuer une communication qui a été initialisée.**
  - La seconde régle autorise tous les hôtes de l'internet (internes ou externes) qui utilisent le numéro de port bien connu à communiquer à condition que le bit ACK soit positionné => on autorise en fait les réponses par un serveur à une communication initialisée en interne.

Règle	IP Source	Port Source	IP Dest	Port Dest	Complément
Autoriser	Mes-hotes	*	*	Service-TCP	TCP
Autoriser	*	Service-TCP	*	*	TCP, ACK

Conclusion
Avantages des filtres de paquets

- **Un filtre de paquets peut protéger** en un seul dispositif tout un réseau d'entreprise.
- **La mise en place du filtre peut être réalisée** par l'équipe système indépendamment des usagers qui gèrent les postes clients ou serveurs.
- **Les filtres de paquets sont très répandus**
  - dans tous les routeurs
  - sous forme de logiciels filtres logiciels libres ou propriétaires.

Conclusion : Inconvénients des filtres de paquets

- **Le filtrage de paquets pose des problèmes de mise en oeuvre.**
  - Règles difficiles à définir.
  - Règles difficiles à assembler en une suite cohérente.
  - Fonctionnalités des filtres dont on dispose spécifiques ou incomplètes ou difficiles à comprendre.
- **Certains protocoles applicatifs posent des problèmes pour le filtrage**
  - Exemples : utilisation de ports alloués dynamiquement.
- **Les filtres de paquets ne prennent pas en compte les données des applications**
  - Exemple: filtrer sur le nom d'un usager dans un accès distant ou dans un transfert de fichier.
  - Nécessité de mettre en œuvre des proxys.

Bibliographie : Pare-feux

- D. Brent Chapman, Elisabeth D. Wwicky '**La sécurité sur Internet Firewalls**' O'Reilly , 1996.
- William R. Cheswick, Steven M. Bellovin, '**Firewalls and Internet security**', Addison Wesley, 1994.