



Principes d'architecture sécurisée

*Premier Maître Jean Baptiste FAVRE
DCSIM / SDE / SIC / Audit SSI
jean-baptiste.favre@marine.defense.gouv.fr*



Au menu

➔ Un peu de théorie...

- Principes de sécurité
 - Le moindre privilège
 - Défense en profondeur
 - Goulet d'étranglement
 - Le maillon le plus faible
 - Position de panne sans danger
 - Diversité de défense
 - Unicité de fonction

➔ ... et de pratique

- Du plus simple...
- ... au plus complexe



Théorie: Le moindre privilège

- ➔ **Moins on a de droit, moins on fera de bêtise**
 - Pas besoin d'être root pour **consulter** les journaux de log
 - L'utilisateur root n'a pas besoin d'accéder à Internet (sauf pour les mises à jour)
 - Un serveur ne devrait jamais tourner en tant que root
 - Tout ce qui n'est pas explicitement autorisé est interdit

Théorie: Défense en profondeur

- ➔ Il faut se protéger à tous les niveaux où l'on peut intervenir
 - Couches réseaux (logique)
 - Filtre de paquets (paramétrage redondant et/ou complémentaire)
 - Relais applicatifs
 - Machines (physique)
 - Serveurs
 - Firewall
 - Postes clients
 - Locaux (physique)
 - Accès, incendie, alimentation, climatisation, ...



► N'offrir qu'un seul accès depuis et vers l'extérieur

- Chasser les accès ADSL « pirates » (non contrôlés) à l'intérieur de votre réseau
- Attention aux nomades (Blaster, nimda, ...)
- Les VPN, c'est bien, mais il faut contrôler tous les réseaux qui y participent.

Théorie: Le maillon le plus faible

- ▶ **La solidité de votre architecture de sécurité correspond à celle du maillon le plus faible**
 - Suivi des serveurs (mises à jour de sécurité)
 - Failles intrinsèques de certains protocoles (SSH inutile si telnet activé)
 - Attention à la machine d'administration de l'architecture (elle est par définition sensible)


Théorie: Panne sans danger

- **Si un service s'arrête, l'accès doit être refusé**
 - Exemple d'un filtre de paquet qui, lorsqu'il s'arrête, laisse passer tout le trafic, quel qu'il soit
- **Impose une réactivité pour rétablir l'accès aux utilisateurs légitimes**
- **Implique une politique par défaut**
 - Refus par défaut
 - Devrait être votre vision
 - Autorisation par défaut
 - Sera très certainement celle du client



- **Pour une même fonction, utilisez des systèmes différents**
 - Exemple, mélanger Linux et BSD pour le filtre de paquet, ne pas miser tout sur CISCO, ...
 - Gourmand en compétence système
 - Complique la tâche d'un attaquant pour la même raison.
 - Intégration parfois problématique (administration, journalisation, ...)

Théorie: Unicité de fonction

- 
- ➔ **Moins on en fait, mieux on se porte !!**
 - Une fonction, une machine
 - Réduction de la surface d'attaque
 - La compromission d'un service ne met pas en péril l'ensemble de l'architecture

Théorie: Conclusions

- **Le respect de chacun de ces principes augmente sensiblement le niveau de sécurité**
- **Mais:**
 - Ne vous met pas à l'abri des attaques
 - Complexifie l'architecture et augmente le risque de non maîtrise
- **Le principal facteur de choix est bien souvent le budget**

Le budget: élément limitant ?

➔ Critères:

- Logique
 - Par couches réseaux
- Sensibilité
 - Le serveur VPN doit être seul à bord
 - Le dernier filtre de paquet avant le réseau local aussi.
 - Les proxy peuvent être « mariés »
 - Les anti-virus aussi
- Psychologique
 - Impliquer les utilisateurs dans la définition du cahier des charges

... et de pratique

- **Le principal écueil est (volontairement) écarté**
 - Il faut se donner les moyens de sa sécurité
 - Ou en tout cas, faire au mieux
 - En fonction de la politique de sécurité de l'entité
 - Et de l'analyse de risques
- **Le second aussi**
 - Prévoir la formation des administrateurs
 - Assurer le suivi de l'infrastructure
 - Définir les procédures en cas de problème
 - ...
- **Bref, s'organiser**



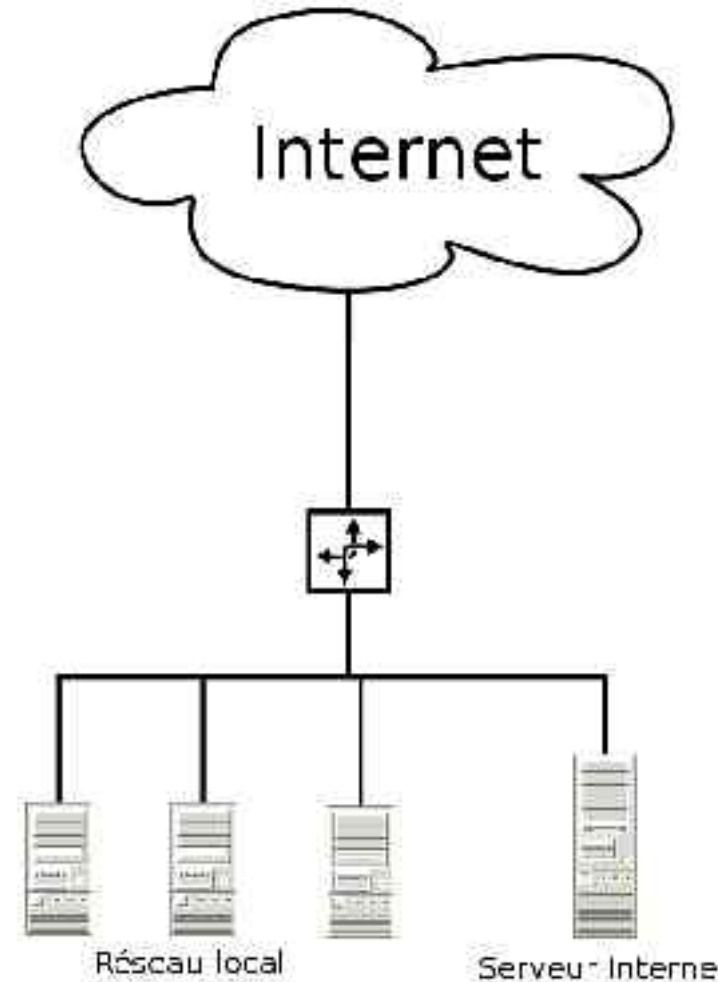
Routeur seul

➔ Avantages:

- Simple et peu cher
- Convient à tous les trafics
- Bonnes performances
- Fonctionnalités étendues

➔ Inconvénients

- Couche internet seulement
- Vulnérable à l'usurpation IP
- Ressources parfois limitées
- Journalisation peu évoluée
- Tout en un



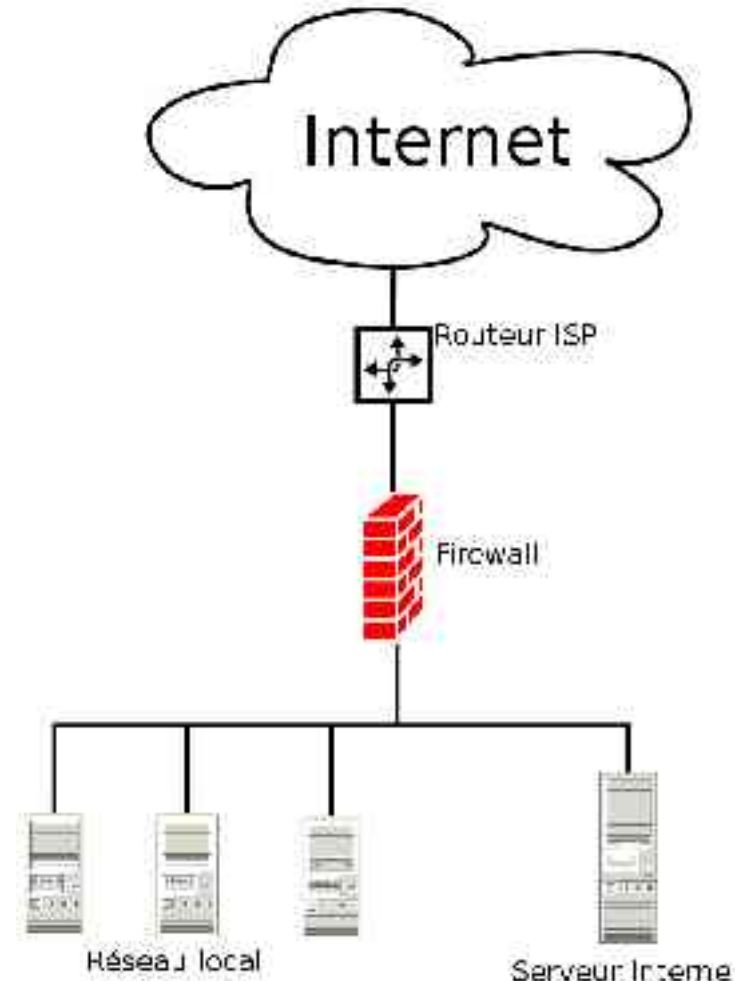
Routeur et Filtre de paquets

➤ Avantages

- Simplicité
- Séparation des tâches
- Gestion de la couche Transport
- Usurpation d'IP impossible
- NAT et normalisation de paquets

➤ Inconvénients

- Couche applicative non gérée
- Pas de DMZ



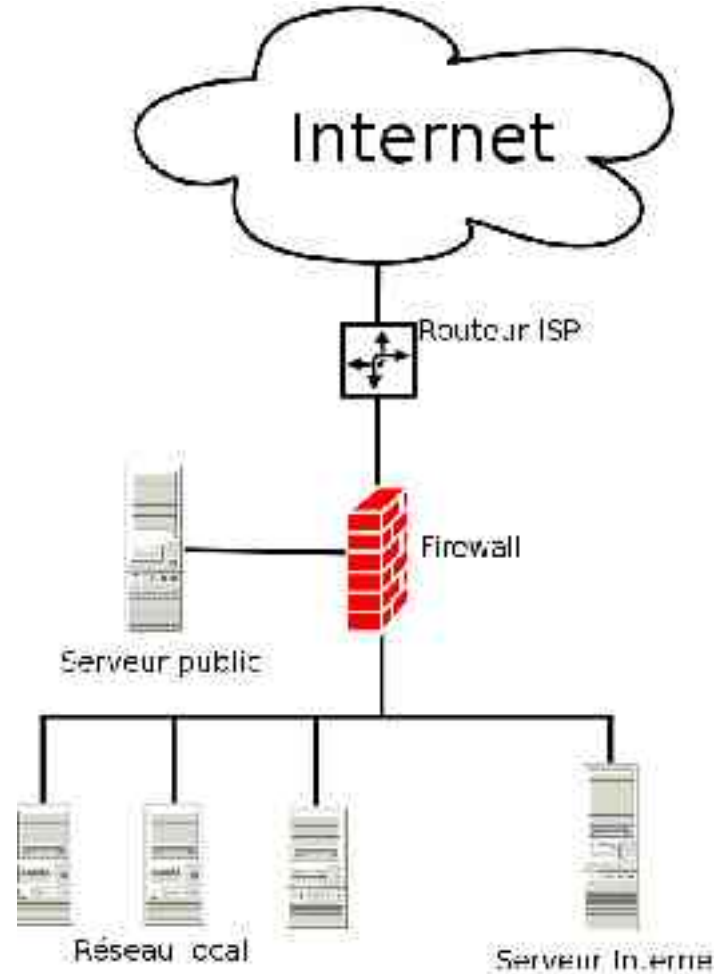
Routeur, Filtre de paquet et DMZ

➤ Avantages

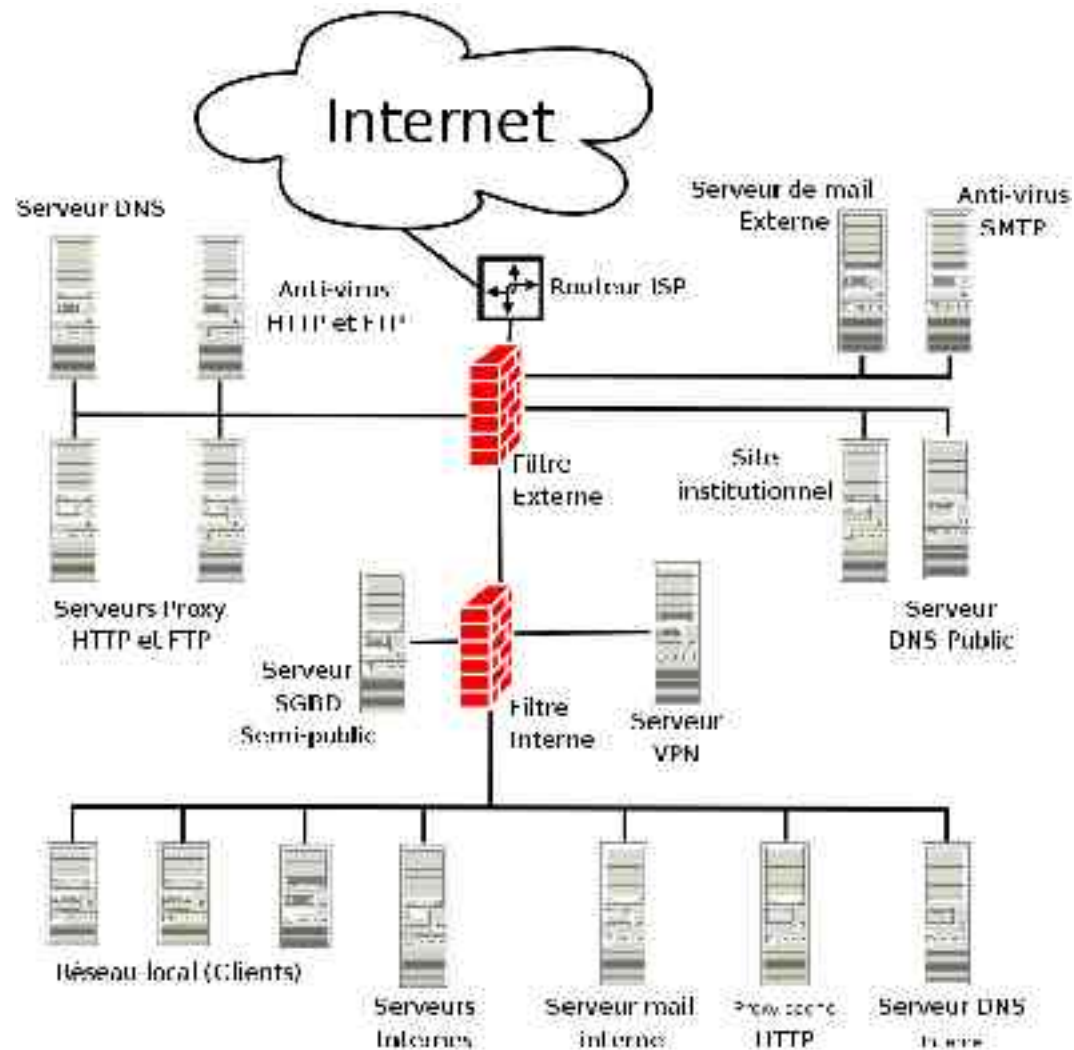
- DMZ
- Filtrage couche applicative
- Cloisonnement plus important
- Contrôle de l'accès internet

➤ Inconvénients

- Pas d'accès distant
- Un seul filtre de paquets
- Pas de séparation flux entrants / sortants
- Administration



La totale: Le Saint-Graal



La totale: avantages

➔ Avantages

- Séparation des flux entrants / sortants
- Analyse des flux à tous les niveaux (MAC, IP, TCP/UDP/ICMP, Applications)
- Contrôle maximal de l'accès vers Internet
- Contrôle maximal de l'accès depuis Internet
- Authentification forte des nomades et/ou partenaires (VPN)
- Pas de maillon faible unique
- La journalisation peut être très fine
- Hiérarchisation de la sensibilité des flux (DMZ différentes)

La totale: inconvénients

➔ Inconvénients

- Coût
- Difficulté de mise en œuvre
- Charge en terme d'administration
 - Compétence selon les technologies
 - Corrélation et analyse des logs
- Complexité = difficile à maîtriser
 - Règles de filtrage
 - Cohérence des configurations



La totale: Journalisation

➔ Fonctions

- Journalisation centralisée
- Choix des équipements
- Réseau dédié journalisation et administration
- Serveur dédié

➔ Avantages

- Isolement de l'administration du réseau principal
- Pas de problème de bande passante
- Pas d'interaction entre réseaux

➔ Inconvénients

- Réseau dédié / Serveur dédié = plus cher
- Règles supplémentaires sur les routeurs / filtres

La totale: IDS/IPS

➔ Avantages

- Surveillance plus serrée de l'infrastructure et du trafic
- Réactivité plus importante
- Mieux si réseau dédié

➔ Inconvénients

- Demande une permanence H24
- Compétences très pointues pour les analyses
- Corrélation délicate avec les logs des équipements
- Demande une très bonne maturité SSI
- Risque de réaction disproportionnée si mauvaise analyse

La totale: comment faire ?

- Politique de sécurité
- Besoin d'interconnexion
- Besoin en bande passante
- Diagramme de flux
- Configuration des équipements
 - Matériel (performances)
 - Logiciel (sécurisation OS)
- Configuration des clients (nomades)
 - Logiciel (sécurisation OS)



Questions ?