MINISTÈRE
DE LA DÉFENSE

Mise en place

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

sersim

MINISTÈRE
DE LA DÉFENSE

Au menu

- Cahier des charges fonctionnel
- Définition de l'architecture
- Cahier des charges technique
  - Plan d'adressage IP
  - Diagramme des flux
- Présentation de Netfilter sous Linux
- Compilation du diagramme de flux
- Et après ?

sersim

Cahier des charges fonctionnel

- Accès vers Internet
  - Transfert de fichiers
  - Consultation de sites Web
  - Envoi et réception de mails
  - Administration à distance
- Accès depuis Internet
  - Site institutionnel dynamique
  - Dépôt de mails
  - Accès VPN

MINISTÈRE
DE LA DÉFENSE

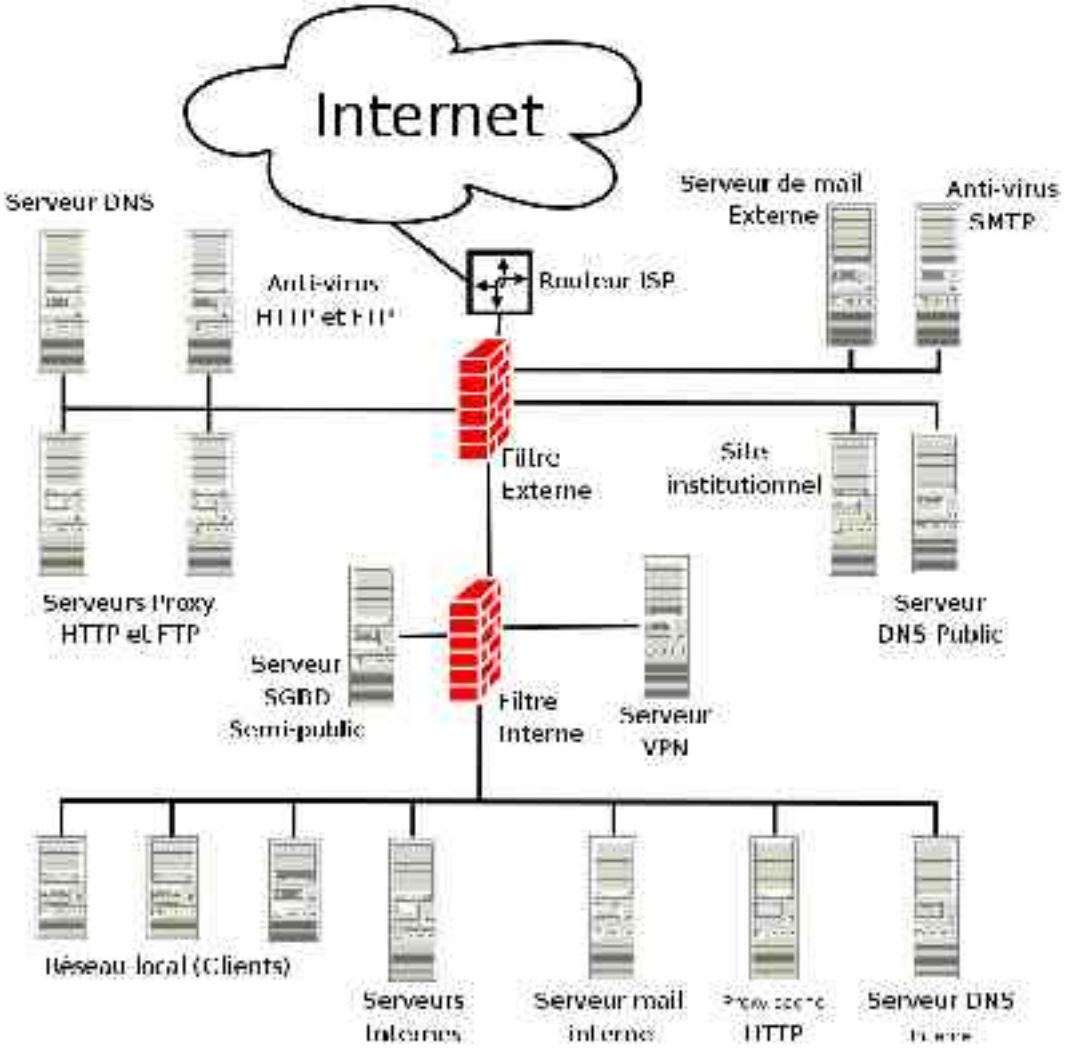
Cahier des charges technique

- Diagramme de flux
  - Faire apparaître les connexions inter-DMZ
  - Faire apparaître les flux « sensibles »
    - Plus le diagramme de flux sera détaillé et générique, plus les règles des filtres de paquets seront faciles à mettre en place
- Plan d'adressage IP
  - Segmentation maximale
  - Identifier les besoins de translation d'adresses
- Fonctionnalités du filtre de paquets
  - NAT
  - Modification dynamique de paquets

sersim

MINISTÈRE
DE LA DÉFENSE

Le « Saint-Graal » de la SSI



MINISTÈRE
DE LA DÉFENSE

Diagramme de flux

Vers / De	Réseau local	DMZ SGBD	DMZ VPN	DMZ Sortante	DMZ Mail Externe	DMZ Publique	Internet
Réseau local		Selon SGBD Administration	Administration	HTTP HTTPS FTP DNS Administration	POP3 SMTP Administration	HTTP HTTPS FTP Administration	
DMZ SGBD							
DMZ VPN	Partage de fichiers Domaine Windows DNS POP3 SMTP	Selon SGBD		HTTP HTTPS FTP	POP3 SMTP	HTTP HTTPS	
DMZ Sortante							HTTP HTTPS FTP DNS
DMZ Mail Externe				DNS HTTP			SMTP
DMZ Publique		Selon SGBD					
Internet			IPSEC			HTTP DNS	

MINISTÈRE
DE LA DÉFENSE

Plan d'adressage IP

- Une répartition « arbitraire »
  - Réseau local: 192.168.0.0/24
  - DMZ:
    - SGBD: 192.168.10.0/30
    - VPN: 192.168.10.4/30
    - Sortante: 192.168.10.8/29
    - Mail: 192.168.10.16/29
    - Publique: 192.168.10.24/29
  - Filtres de paquets: 192.168.20.0/30

sersim

MINISTÈRE
DE LA DÉFENSE

Adressage IP détaillé

Filtre de paquets	IP / Interfaces	Masque	Routes	Nb IP
Interne	192.168.0.1	255.255.255.0	* -> 192.168.20.2	253
	192.168.10.1	255.255.255.252		1
	192.168.10.5	255.255.255.252		1
	192.168.20.1	255.255.255.252		1
Externe	192.168.20.2	255.255.255.252	192.168.0.0 -> 192.168.20.1 192.168.10.0 -> 192.168.20.1 192.168.10.4 -> 192.168.20.1 * -> Passerelle FAI	0
	192.168.10.9	255.255.255.248		5
	192.168.10.17	255.255.255.248		5
	192.168.10.25	255.255.255.248		5
	DHCP FAI	DHCP FAI		
Serveur SGBD	192.168.10.2	255.255.255.252	* -> 192.168.10.1	0
Serveur VPN	192.168.10.6	255.255.255.252	* -> 192.168.10.5	0
Proxy HTTP sortant	192.168.10.10	255.255.255.248	* -> 192.168.10.9	4
Proxy FTP sortant	192.168.10.11	255.255.255.248	* -> 192.168.10.9	3
Proxy DNS	192.168.10.12	255.255.255.248	* -> 192.168.10.9	2
Anti-virus HTTP-FTP	192.168.10.13	255.255.255.248	* -> 192.168.10.9	1
Serveur Mail	192.168.10.18	255.255.255.248	* -> 192.168.10.17	4
Anti-virus SMTP	192.168.10.19	255.255.255.248	* -> 192.168.10.17	3
Serveur Web public	192.168.10.26	255.255.255.248	* -> 192.168.10.25	4
Serveur DNS public	192.168.10.27	255.255.255.248	* -> 192.168.10.25	3

sersim

MINISTÈRE
DE LA DÉFENSE

Politique de sécurité

- Esquisse des responsabilités
- La liste exhaustive des flux autorisés
  - Attention aux boulettes:
    - Les flux HTTP impliquent le DNS !!

La politique de filtrage doit être issue de ce document

- Elle ne doit pas donner de détails techniques
  - Proxy, relais, ...

sersim

MINISTÈRE
DE LA DÉFENSE

Procédures de sécurité

- Procédures de mises en place
  - Doivent décrire l'architecture et justifier l'utilisation de moyens techniques particuliers (proxy, anti-virus, ...)
  - Évoluent en même temps que le système.
- Les procédures d'exploitation et de sécurité
  - Qui fait quoi, comment
    - Exploitation des journaux de log
    - Réactions face à une attaque
    - Formations des opérateurs
  - Niveau de responsabilité
    - Qui décide de couper ?

sersim

Mise en place

Questions ?