PRÉSENTATION DU MÉTIER D'INTÉGRATEUR

Intégration de réseaux et systèmes sécurisés pour l'aviation civile

Aurélien Bouzon

Ingénieur sécurité réseaux et systèmes

TLS-SEC

08/01/2019

Plan

I. PRÉSENTATION

1. La société de service

Société de Service en Ingénierie Informatique (**SSII**)

↓

Entreprise de Services du Numérique (**ESN**)

Gammes de service :

- ➔ Conseil / Assistance
- ➔ Intégration
- ➔ Infogérance

Offre une forte diversité de missions ce qui permet d'appréhender beaucoup de milieux / technologies en « peu » de temps

Beaucoup, beaucoup de concurrence :

Capgemini, Atos, IBM, Accenture, Steria, OBS, CGI, GFI, Econocom …

Les certifications

un business, une reconnaissance par les entreprises

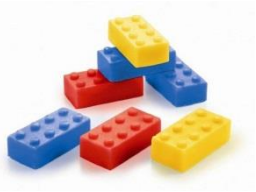
Certifications sécurité de consultants Atos	Nombre
CISSP	129
CISA	31
CISM	24
Certified Ethical Hacker CEH	21
ISO 27001 Lead Auditor	48
BSI IT Grundschutz	6
PCI DSS QSA	6
Other Security related certifications	355
Total	620

2. Le métier d'intégrateur

Le travail d'un intégrateur

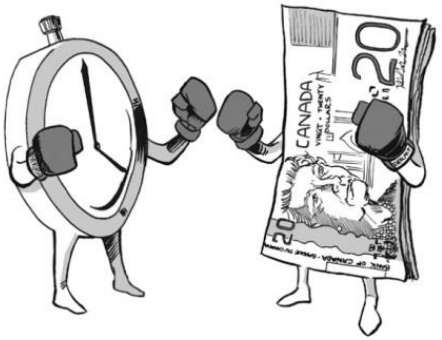
- **AMO(A)** : Assistance à Maitrise d'Ouvrage
  - → conseil, accompagnement, expertise technique
  - → pilotage, gestion de projet

- **Intégrateur** : sélectionner et assembler des briques système (software ou hardware) pour répondre à un besoin client.

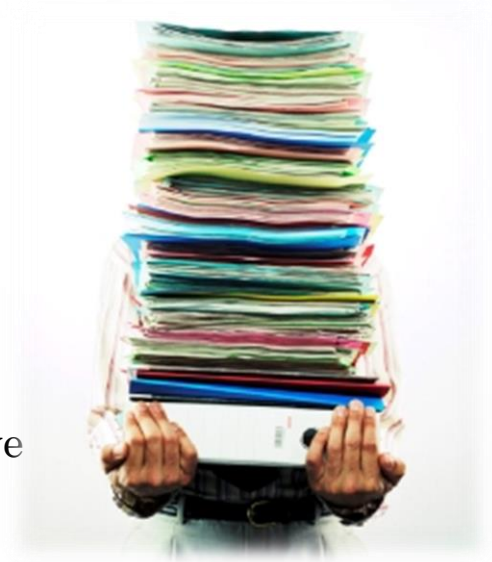


1. Découverte de l'environnement client
2. Recueil du besoin client (contexte client)
3. Proposition de solutions (coût / complexité)
4. Développement / intégration
5. Test / validation
6. Déploiement
7. Support

- Un projet doit être réalisé dans les temps
  - → importance du chiffrage des activités
  - → pas de retard pour éviter l'insatisfaction client
  - → pas de retard pour ne pas perdre d'argent



I. Présentation
2. Le métier d'intégrateur
Les livrables

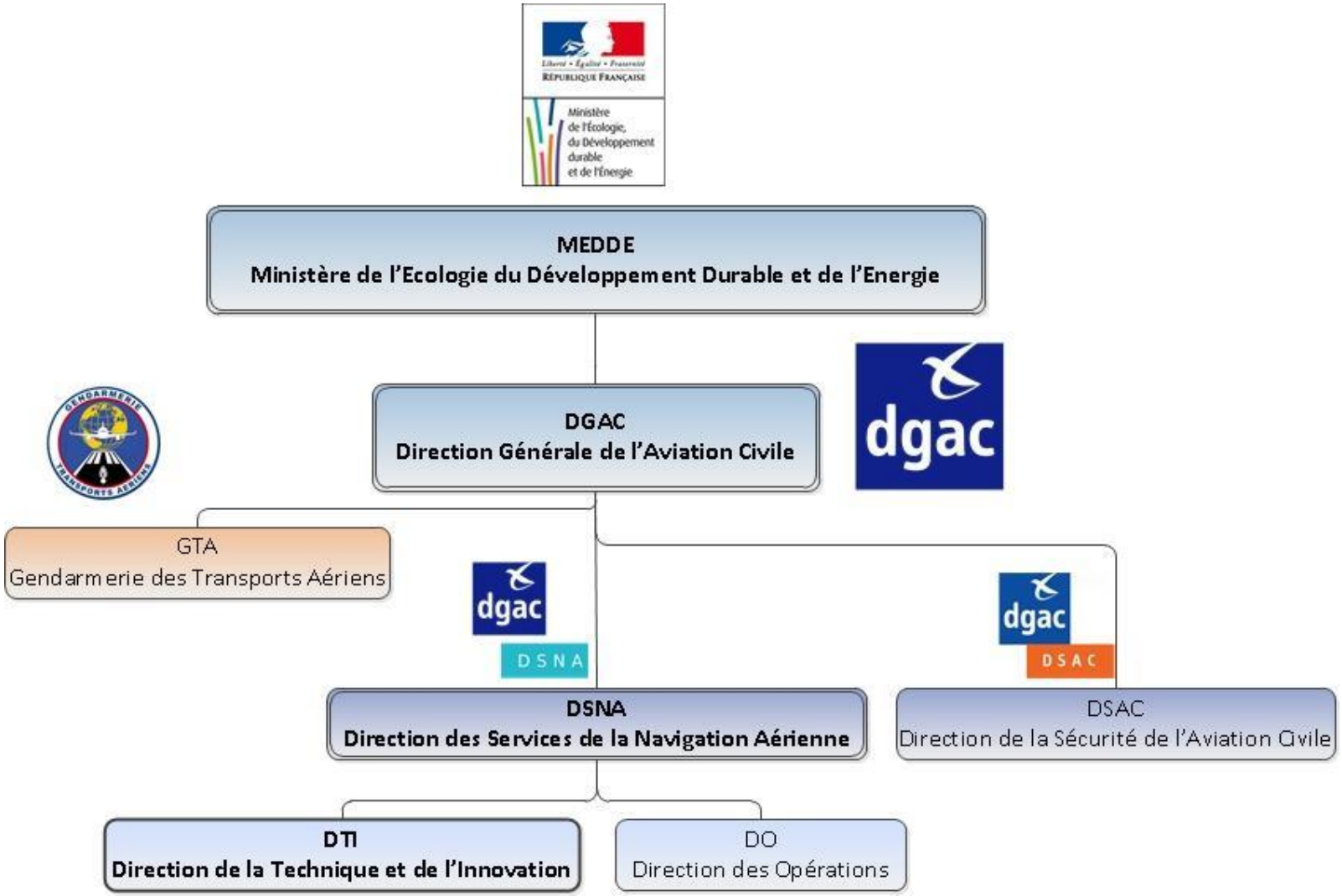


- **Des livrables à produire :**
  - Cahier des charges / Exigences
  - Etudes préliminaires de faisabilité
  - Comparatif et test de produits / Etude comparative
  - Etude d'architecture / Etude d'évolution
  - Revues client
  - Dossier d'architecture / Dossier de conception
  - Dossier de tests / Dossier de validation / Dossier de recette usine
  - Manuels d'utilisation / Manuels d'installation
  - Documents liés à la conduite de projets (compte rendu de réunion, recadrage du projet …)
  - Eventuellement un produit logiciel ou matériel
  - Gérer les phases de migrations
  - … et bien d'autres

→ Souvent beaucoup de documentation

→ La documentation annexe est en général aussi conséquente, sinon plus, que le produit fini lui même

I. Présentation
3. Aviation Civile
Organigramme



I. Présentation
3. Aviation Civile
La DSNA

dgac

DSNA

Prestataire de service de la Navigation Aérienne

- Fournit les services permettant le bon déroulement de l'activité de contrôle aérien.

- Echanges avec :
  - des partenaires Européens
  - des partenaires mondiaux (DOM/TOM)
  - des partenaires industriels
  - des compagnies aériennes
  - des gestionnaires d'aéroport
  - Météo France
  - L'armée
  - Les usagers
  - …

EUROCONTROL

Aena Aeropuertos Españoles y Navegación Aérea

Belgocontrol

DFS Deutsche Flugsicherung

skyguide

ENAIRE

NAV CANADA

FEDERAL AVIATION ADMINISTRATION

AÉROPORTS DE PARIS

AIRFRANCE

AÉROPORTS de LYON

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE LA DÉFENSE

METEO FRANCE

I. Présentation
3. Aviation Civile
La DTI

- Missions : définir, faire réaliser et installer les systèmes techniques utiles au contrôle Aérien.

Radar :
- Primaire : pulse / echo
- Secondaire : transpondeur
- Air
- Sol
- Multilatération

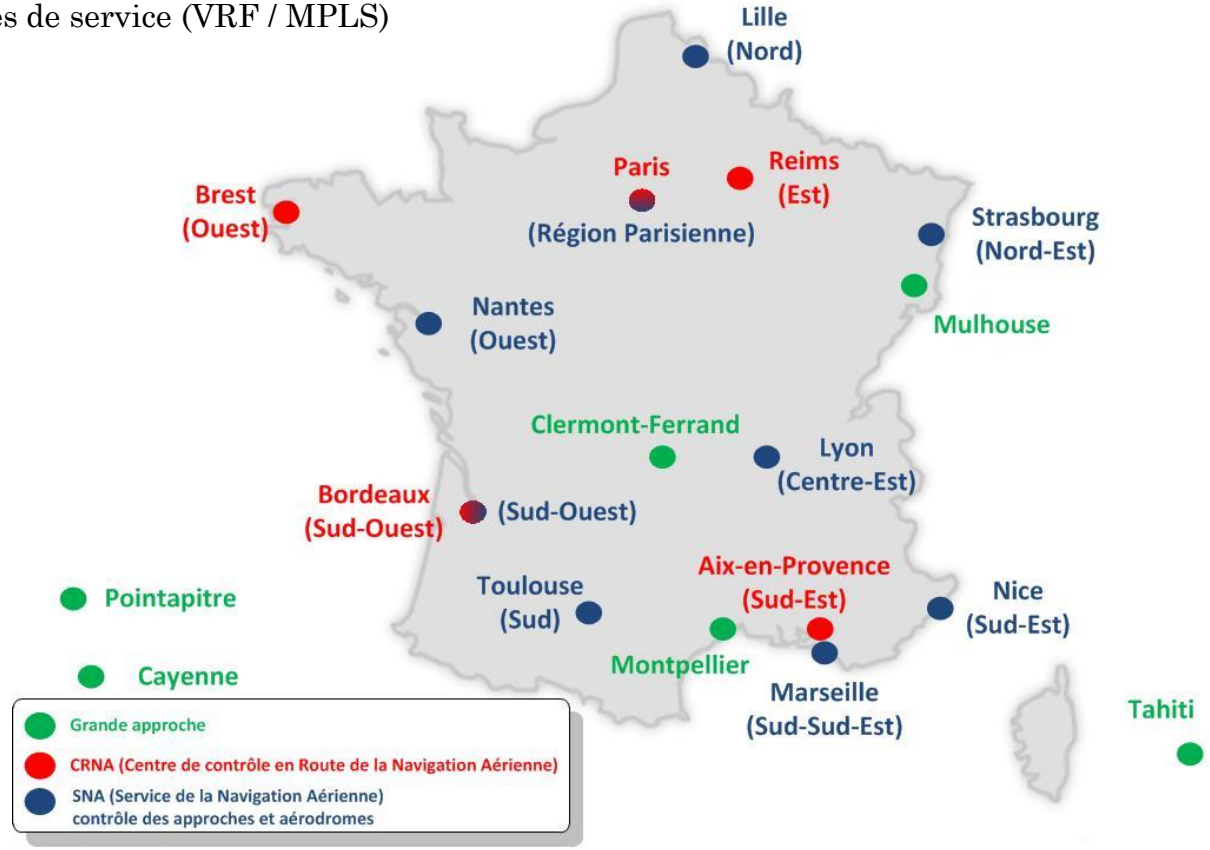
Assistance au contrôle
- écran RADAR
- Strips
- messagerie aéronautique
- Téléphonie
- DMAN (Départure Manager)
- AMAN (Arrival Manager)

Assistance au pilotage
- Radio
- VOR
- DME
- ILS

Réseau
- WAN
- LAN
- Supervision
- Sécurité

I. Présentation
3. Aviation Civile
Un Réseau national : RENAR IP

- Réseau national, remplaçant le réseau RENAR (X25), qui véhicule les données du transport aérien
- Eviter les points de défaillance unique (SPoF : Single Point of Failure)
  - Réseau maillé
  - S'appuie sur plusieurs opérateurs et arrivées (indépendance des arrivées et des chemins)
  - Exploitation d'une longueur d'onde (lambda)
  - Classes de service (VRF / MPLS)



Plan

I. Présentation
II. **Contexte / Enjeux**
III. Aspects réglementaires
IV. Architecture réseau
V. Cas d'application
VI. Durcissement système
VII. Intégration système
VIII. Cadre organisationnel
IX. Conclusion

II. Contexte / Enjeux
Pourquoi de la sécurité pour la DSNA ?

L'aviation civile passe d'un monde fermé à un monde de plus en plus "ouvert"

Informations sur le trafic aérien (accessibles pas construction)

- Radio
- Horaires des vols / quasi temps réel (tableau d'affichage aéroport)

Sur Internet (partage de l'information)

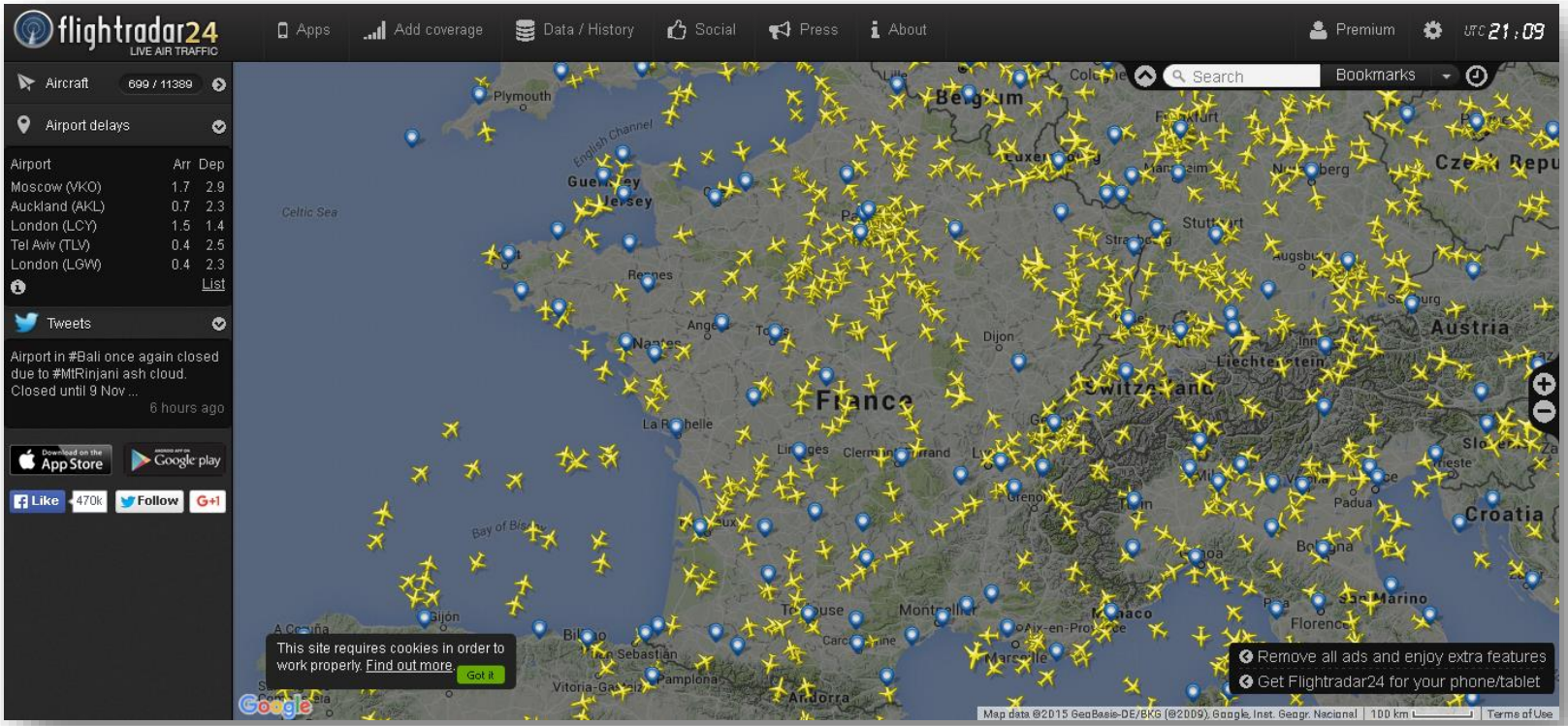
- **ADS-B**
- **Dépose de plan de vol / Actualité aéroportuaire**

Dans l'avion (toujours plus connecté)

- Internet en vol par satellite et station de base au sol
- Wifi (divertissement et information d'exploitation)
- Ecran de divertissement dans l'avion (souvent un linux intégré)

II. Contexte / Enjeux
ADS-B

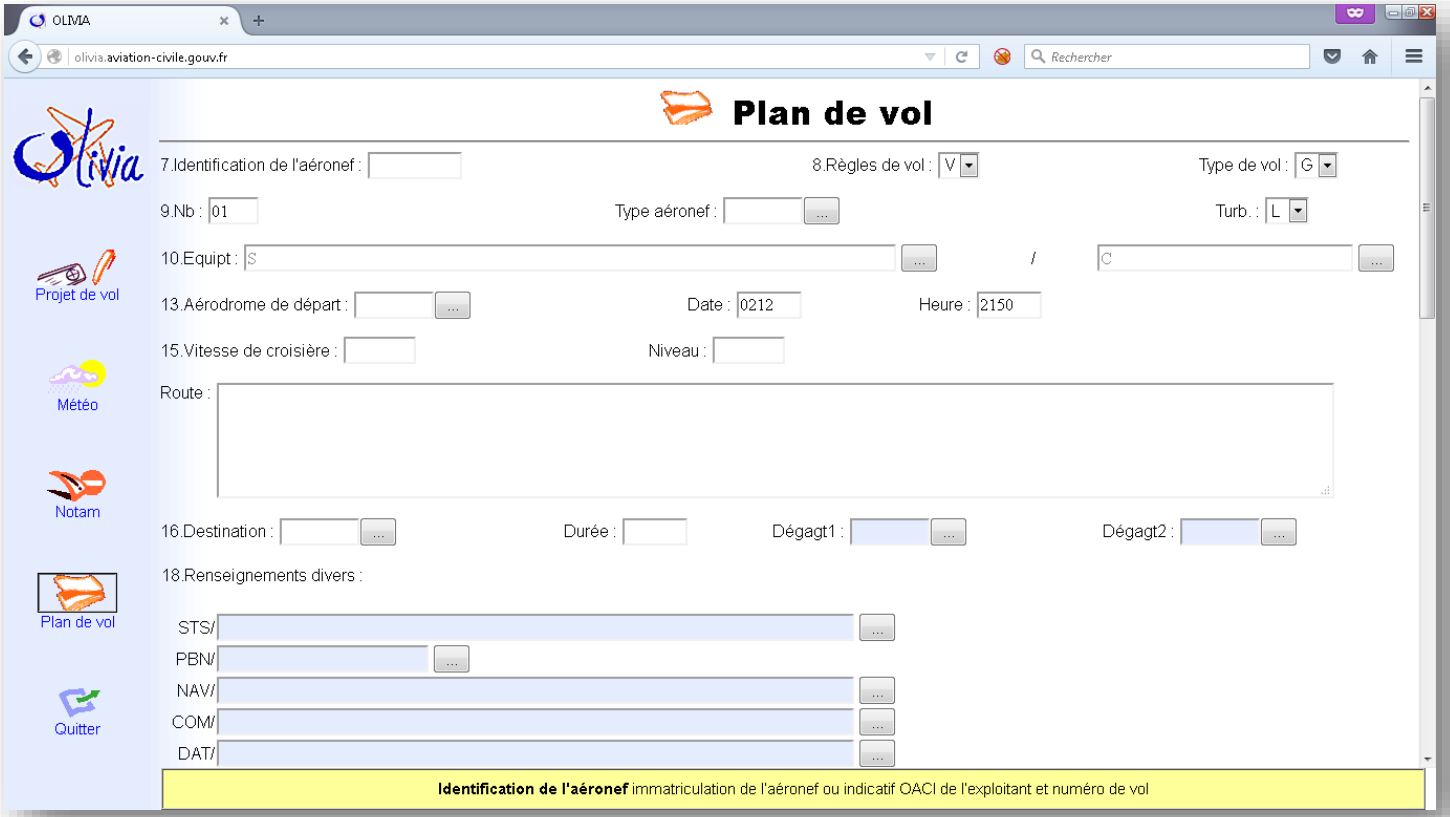
- Diffusion de l'information par l'avion (position, vitesse, direction)
  - Corruption possible → créer un avion en diffusant des informations
  - Information très précise (trop ?)
  - Système conçu avant tout pour être fonctionnel, la sécurité n'était pas une priorité lors de la conception



II. Contexte / Enjeux
Plan de Vol

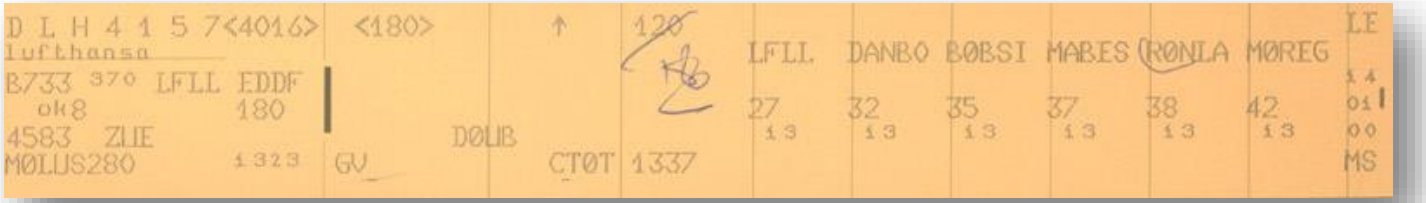
- Dépose libre sur Internet
- Notam (Notice to Airmen) : informations aux navigants

➔ Service en ligne Olivia (http://olivia.aviation-civile.gouv.fr/)



II. Contexte / Enjeux
Gestion électronique

- Avant, tout était géré sous forme papier (plan de vol, stripping, parking)



- Aujourd'hui le stripping est le dernier élément à se dématérialiser

- Système ERATO (En Route Air Trafic Organizer)
  - Optimisation du trafic
  - Couplage à d'autres systèmes pour : économie de kérosène / réduction des retards (DMAN/AMAN)
  - Existence virtuelle de l'avion (plus de strip papier)
  - Des contraintes :
    - Double source électrique
    - Redondance du matériel
    - Duplication de la donnée

- Convergence vers un ciel unique → projet 4Flight

II. Contexte / Enjeux
Quel type de sécurité ?

Confidentialité

- L'aviation civile n'a rien à cacher
- L'information est en très grande partie disponible librement

Authenticité

- **Données radio**
  - Pensée en premier lieu pour la fiabilité de fonctionnement
  - Garantie par le moyen de communication (fréquence radio nécessite une licence)
  - Aucune garantie réelle → protégé par la lourdeur de la sanction
- **Données réseau**
  - Fortes garanties (VPN, liaisons spécialisée)

Intégrité → ce qu'il faut garantir en priorité

- **Données radio** : code OTAN, phraséologie
- **Données réseau** : Réseau propriétaire (engagement contractuel)

Non-répudiation

- Enregistrements légaux (flux radar, plan de vol, radio)

Plan

I. Présentation
II. Contexte / Enjeux
III. **Aspects réglementaires**
IV. Architecture réseau
V. Cas d'application
VI. Durcissement système
VII. Intégration système
VIII. Cadre organisationnel
IX. Conclusion

III. Aspects réglementaires
Statu d'OIV (Opérateur d'Importance Vitale)

D'après le Code de la Défense :

- « gère ou utilise au titre de cette activité un ou des établissements ou ouvrages, une ou des installations dont **le dommage ou l'indisponibilité ou la destruction** par suite d'un acte de malveillance, de sabotage ou de terrorisme risquerait, directement ou indirectement **d'obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation** ;

- ou de mettre gravement en cause la santé ou la vie de la population ».

III. Aspects Réglementaires
Des textes

LPM : Loi de Programmation Militaire

- Les obligations des OIV
  - Notifier l'ANSSI en cas d'incident de sécurité
  - Les modalités de validation / audit (ANSSI)
  - Isoler certains systèmes d'Internet
  - Surveiller son réseau
- Les sanctions en cas de non respect des obligations

ESARR : European Safety Regulatory Requirements

- Harmonisation et l'amélioration de la sécurité au niveau Européen
- Rédigé par Eurocontrol

PSSI : Politique de Sécurité des Système d'Information

- Organisation autour du SI
- Les acteurs
- Les domaines / réseaux / zones et leur rôle (à très haut niveau)
- Les règles d'échange (matrice de flux)
- Les principes généraux spécifiques au métier (focaliser la protection sur ce qui a le plus d'importance)

III. Aspects réglementaires
ANSSI : Agence National de la Sécurité des Systèmes d'Information

Les rôles de l'ANSSI

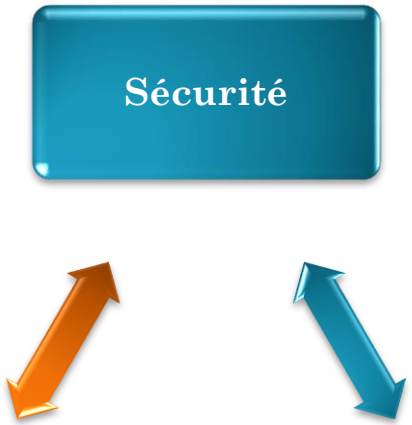
- Conseil / assistance pour les intérêts français :
  - *OIV*
  - *grandes entreprises Françaises*
  - *PME*
- Surveillance / audit (OIV)
- Qualification de matériel (qualifié standard)

Plan

I. Présentation
II. Contexte / Enjeux
III. Aspects réglementaires
IV. **Architecture réseau**
V. Cas d'application
VI. Durcissement système
VII. Intégration système
VIII. Cadre organisationnel
IX. Conclusion

IV. Architecture réseau
Trouver le bon compromis

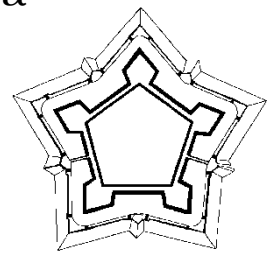
- Bien / vite réagir en cas d'incident → besoin de simplicité
- Besoin de fonctionnalités et d'ergonomie
- Toujours plus de sécurité



IV. Architecture réseau
Définition

Architecture sécurisée

- Manière de structurer le SI pour qu'il soit le plus adapté à l'organisation et au besoin métier
- Repose sur la manière de cloisonner et d'interconnecter
  - Réseaux cloisonnés (segmentation)
  - Réseaux à plat (simple, propagation facilitée)
- Hérite des connaissances militaires (châteaux forts, fortifications de Vauban, prisons, structures panoptiques)



Doit répondre à des problématiques de base :

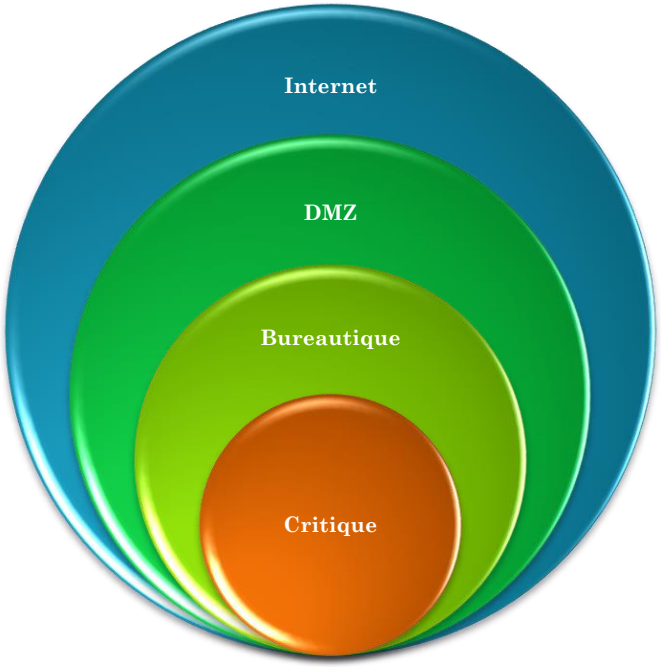
- Débits
- Technologies
- Disponibilité

IV. Architecture réseau
Sécurité périmétrique

Sécurité périmétrique :

- Modèle de protection concentrique
- Chaque niveau de protection est délimité par un élément filtrant (pare-feu)
- Si le périmètre est cassé à un endroit, tout le niveau est corrompu
  - → c'est le maillon le plus faible qui détermine le niveau de sécurité

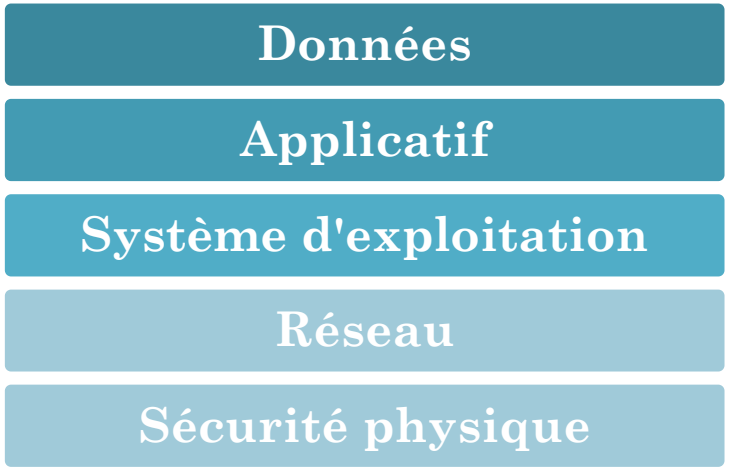
- Le moins critique à l'extérieur
- Le plus critique au centre



IV. Architecture réseau
Défense en profondeur

Sécurité / défense en profondeur

- Sécurisation de toutes les couches OSI "du physique à la donnée"
- Augmente la probabilité de détection d'une attaque
- Diminue les impacts et la vitesse de progression d'une attaque



➔ Actuellement on trouve, le plus souvent, une combinaison des deux approches (périmétrique et en profondeur)

IV. Architecture réseau
La sécurité physique

La sécurité physique poussée à l'extrême

- Isoler le système / réseau de toute interconnexion
- Le placer dans un endroit très protégé (barbelés, bunker, chiens …)

- → Le système / réseau est tellement bien protégé qu'il est inaccessible / inutilisable

- → **La sécurité d'un SI n'est rien sans sécurité physique**
- il est toujours possible de reprendre le contrôle d'un équipement (reset usine)
- → Nécessité du contrôle d'accès

- Favoriser la double authentification
  - Ce que je sais (code)
  - Ce que je suis (biométrie)
  - Ce que je possède (badge)

IV. Architecture réseau
L'ingénierie sociale

Des moyens de "se protéger" de l'humain :

- **Cacher l'information / sécurité par l'obscurantisme** (architecture, type de matériel, procédures …)
- → Permet de **se protéger d'un attaquant extérieur**

- **Formation / sensibilisation contre l'ingénierie sociale**
- → l'ingénierie sociale permet d'obtenir l'information cachée ou un accès
- Pour récupérer l'information **un attaquant externe s'expose / se fait connaître**
- Cacher l'information garde donc un intérêt mais ne peut pas être la seule mesure de protection

- **Habilitation** / surveillance du personnel
- → Permet de **se protéger d'un attaquant interne**

- **Organisation** / segmentation du travail et des connaissances
- → Permet de **se protéger d'un attaquant interne et externe**

IV. Architecture réseau
Les principes de base

Protéger ce qui a le plus de valeur

- Identifier la valeur ajoutée à protéger

Tout ce qui n'est pas autorisé est interdit

Pas d'adjacence de réseau / Pas de double raccordement

- Eviter de raccorder deux zones de criticité différente à un équipement non filtrant → casse la segmentation

Isoler les fonctions / Dédier des systèmes

- A modérer avec l'aspect budgétaire

Maximiser la segmentation / Eviter les réseaux à plat

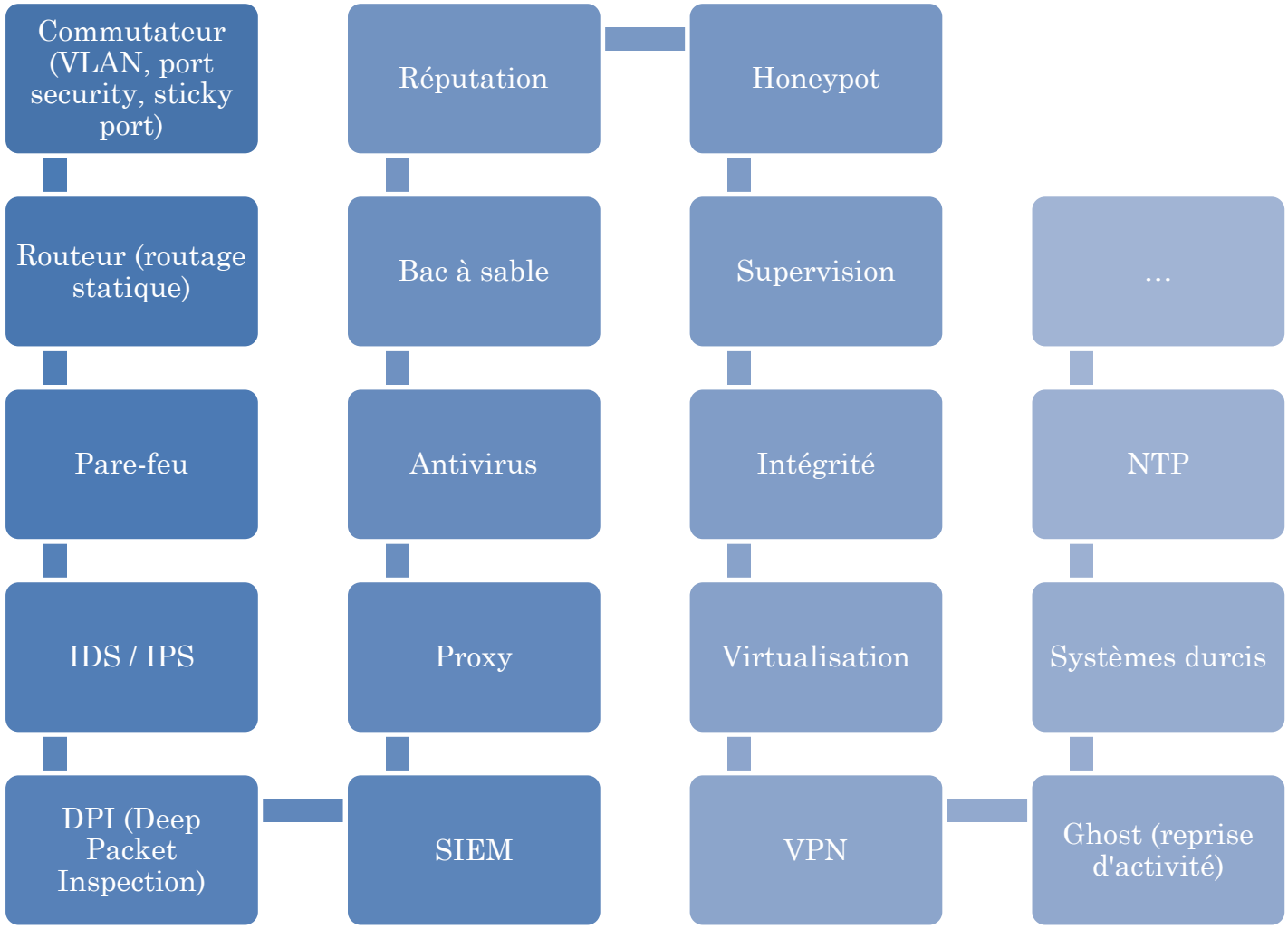
- Compromis : complexité / coût / intérêt
- Permet d'identifier plus facilement les flux (source / destination)

Maximiser les performances de l'architecture

Eviter les points de défaillance unique / Offrir de la disponibilité

- Compromis : besoin / coût
- SPoF : Single Point of Failure
- Mutualiser/ rationaliser

IV. Architecture réseau
Les outils techniques



Plan

I. Présentation
II. Contexte / Enjeux
III. Aspects réglementaires
IV. Architecture réseau
V. **Cas d'application**
    1. **Architecture de base**
    2. **Filtrage applicatif**
    3. **Réplication**
    4. **Disponibilité**
    5. **DoS**
    6. **Détection d'intrusion**
VI. Durcissement système
VII. Intégration système
VIII. Cadre organisationnel
IX. Conclusion

V. Cas d'application
1. Architecture de base
Besoins

Besoins :

- Permettre la dépose des plans de vol depuis Internet
- Récupérer / envoyer des plans de vol de partenaires
- Solution économique

- Segmentation du réseau
- Limiter l'exposition du serveur (services)
- Ne pas donner l'accès au réseau partenaire depuis Internet
- Se protéger de ce qui pourrait venir du partenaire
- Ouvrir les flux à partir d'une matrice de flux identifiée
- Mise en place de règles de filtrage sur un pare-feu
- Masquer l'adresse réelle du serveur (NAT Network Adress Translation) au niveau du pare-feu

V. Cas d'application

1. Architecture de base

Matrice de flux

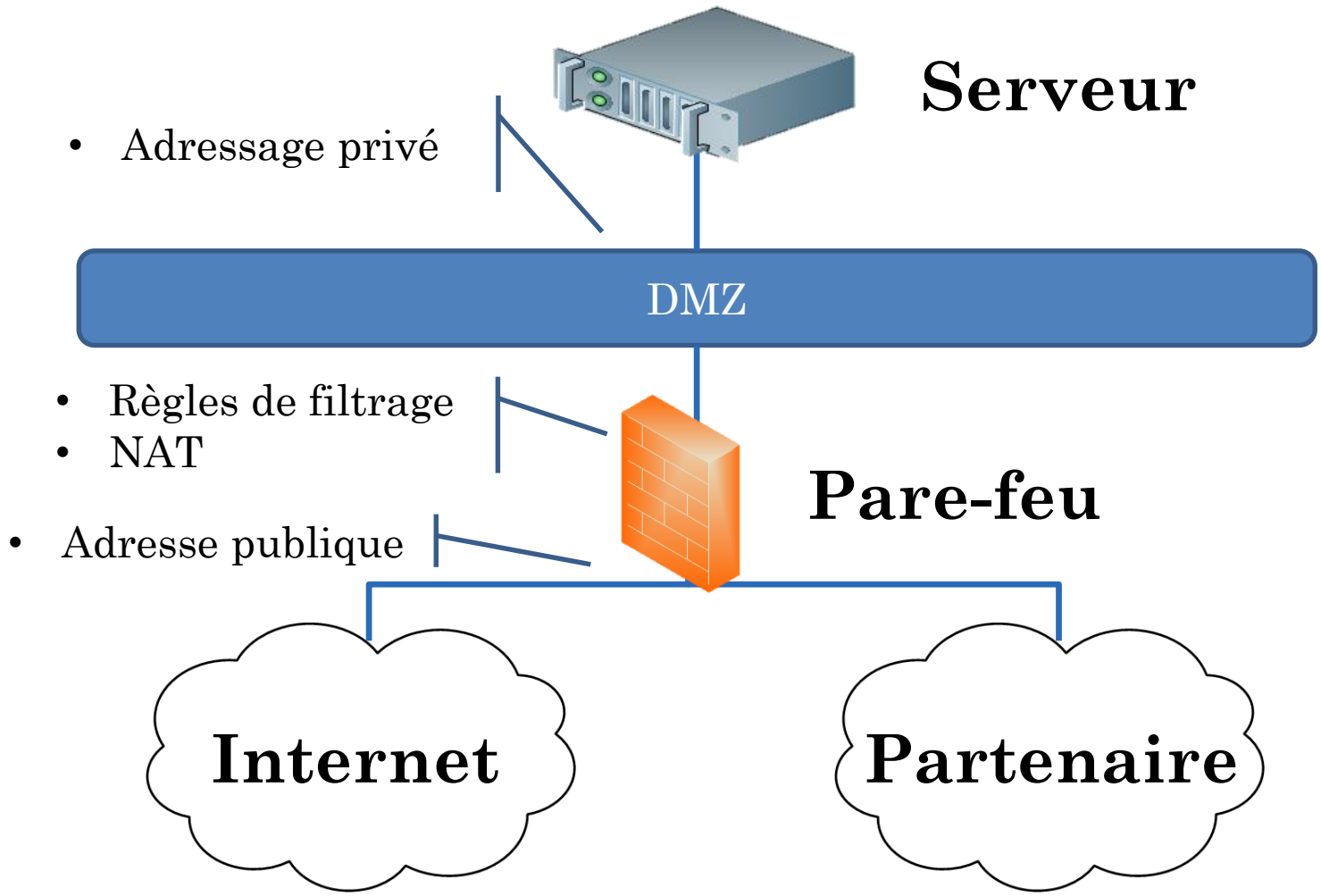
- Le sens d'initialisation d'une connexion importe (TCP SYN ou pseudo connexion UDP)
- La règle dans le sens retour est implicite avec un pare-feu à état (statefull)

Source / destination	Internet	Partenaire	DMZ
Internet			
Partenaire			✓
DMZ	✓	✓	

V. Cas d'application

1. Architecture de base

Schéma



V. Cas d'application
1. Architecture de base
Pare-feu

- Elément de base pour le filtrage entre les réseaux
- Fait une grande partie du travail
  - Règle de filtrage (ACL) niveau 3 et 4
  - NAT
  - Routage
- Existe maintenant sous forme d'appliance virtuelle
- Les appliances physiques ont de meilleures performances ASIC (Application Specific Integrated Circuit)
- Relativement peu d'interfaces (GigaEthernet, Fibre), n'est pas fait pour collecter
- Débit de filtrage limité (quelques giga pour du milieu de gamme)
- Débit souvent limité par les fonctionnalités tierces (antivirus, IPS …)

- Les fabricants proposent aujourd'hui des UTM/USM (Unified Threat/Security Management)
  - IDS/IPS
  - Antispam
  - Antivirus
  - Proxy HTTP
  - Proxy SSL
- Pratique mais va contre le principe de séparation des fonctions (SPoF)

1. Architecture de base

Pas de pub, une vision du marché du pare-feu

V. Cas d'application
2. Filtrage applicatif
Besoins

Besoins :

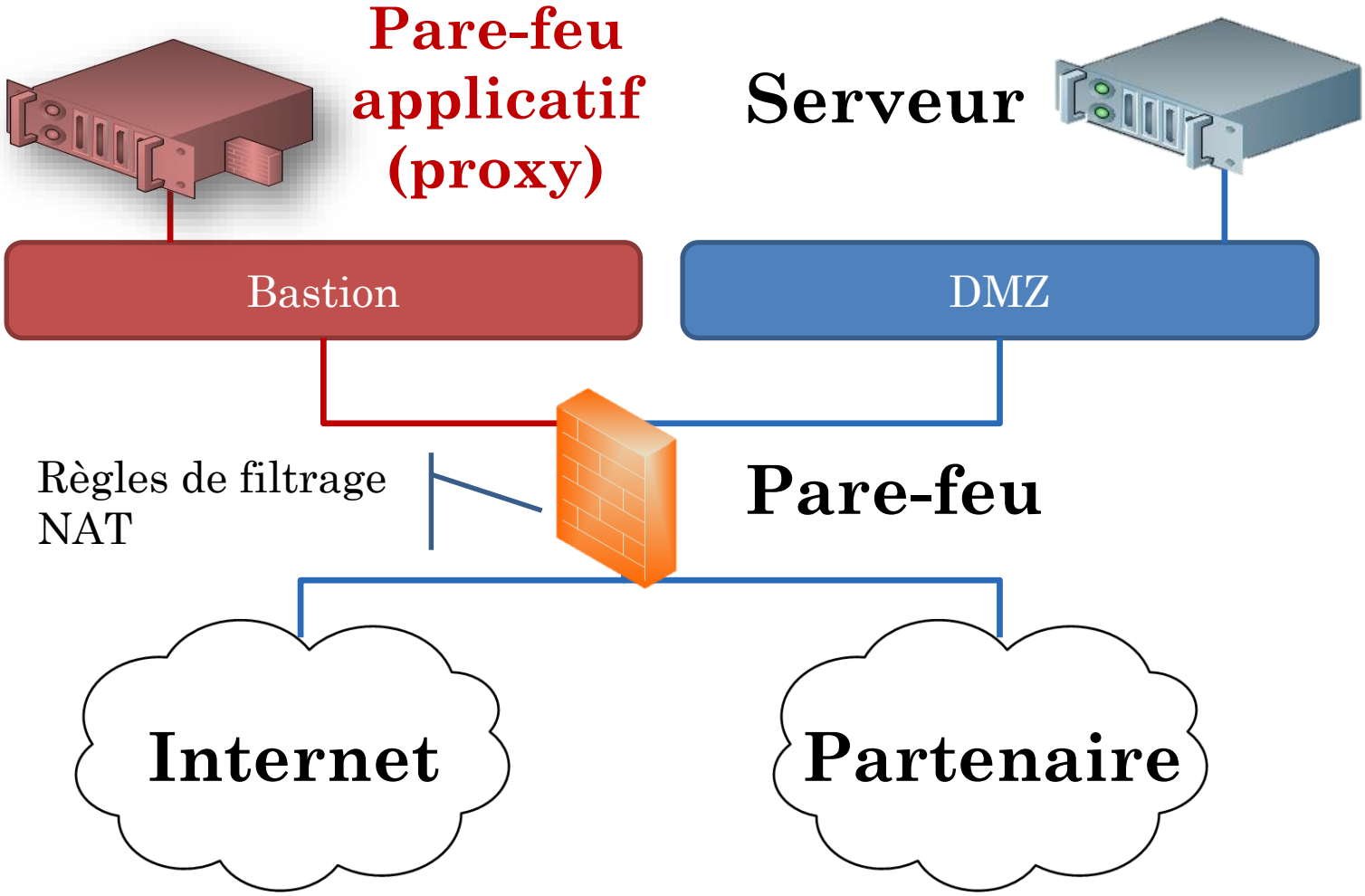
- N'autoriser que les requêtes bien formées

- Réaliser un filtrage de niveau applicatif
- Dédier une machine à ce traitement (proxy)
- Positionner le proxy dans une zone distincte (bastion)

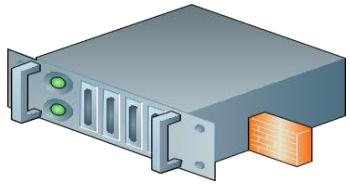
Source / destination	Internet	Partenaire	Bastion	DMZ
Internet				
Partenaire			✓	
Bastion	✓	✓		✓
DMZ			✓	

2. Filtrage applicatif

Schéma



V. Cas d'application
2. Filtrage applicatif
Proxy



Pare-feu de niveau 7 (applicatif)

- Inspecte / filtre la donnée de niveau applicatif
- Réalise une rupture dans la connexion

WAF (Web Application Firewall) = proxy web

- Filtrage URL
- Filtrage paramètres (taille, type, valeur)
- …

Les REGEX sont très utilisées :

- Whitelist/blacklist URL (Pare-feu/Proxy)
- Filtrage de paramètres
- Mais aussi : règle de corrélation (SIEM), Parser (SIEM), IDS, scripting …

Le monde ne se limite pas au web !

- Proxy : SNMP, SYSLOG, NTP, FTP …
- Quid proxy pour protocole non standard / répandu ?
- → Nécessite un développement spécifique

V. Cas d'application
3. Réplication
Besoins

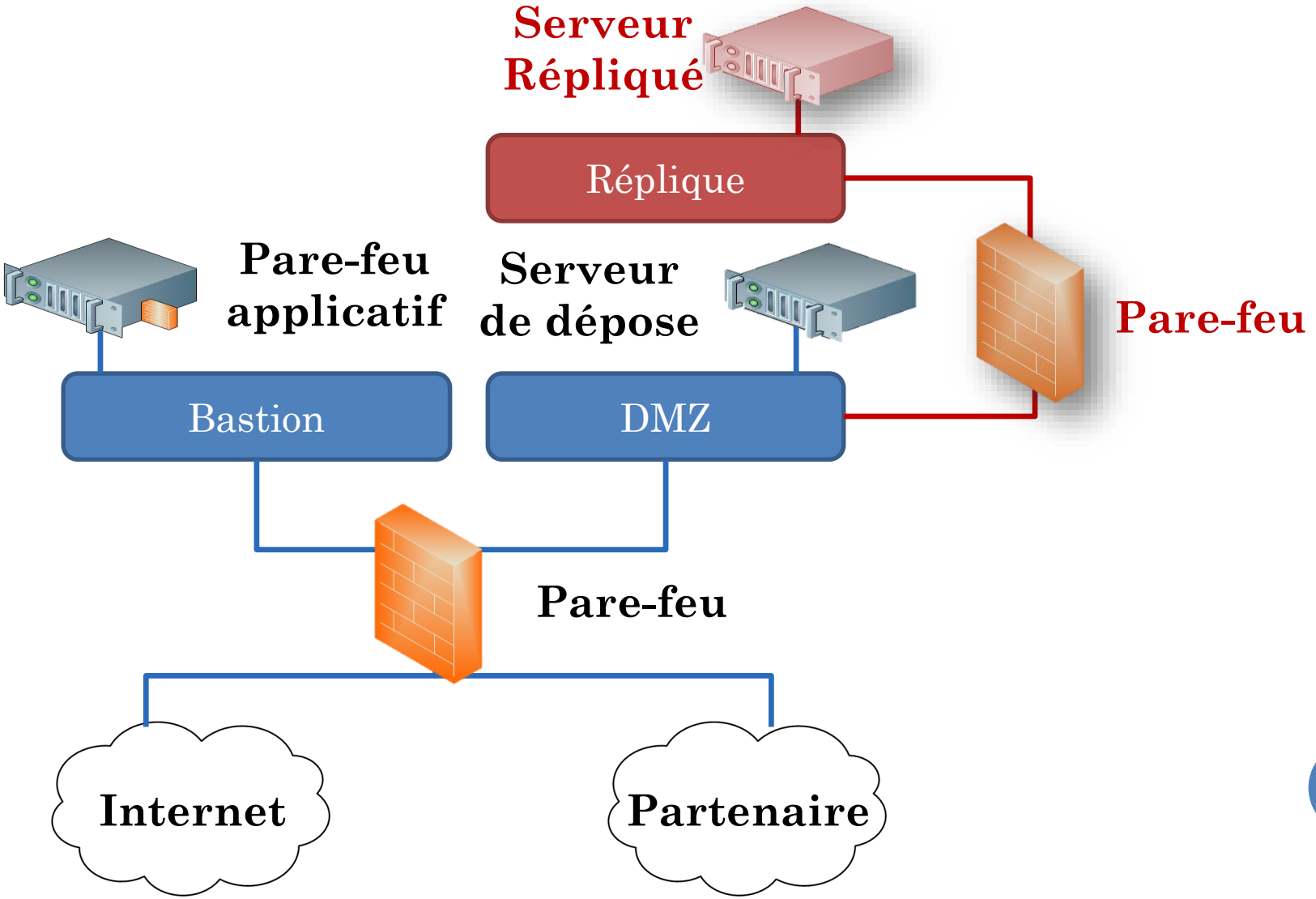
Besoins :

- Empêcher la compromission des plans de vol utilisés pour le contrôle
- Permettre la modération des plans de vol déposés

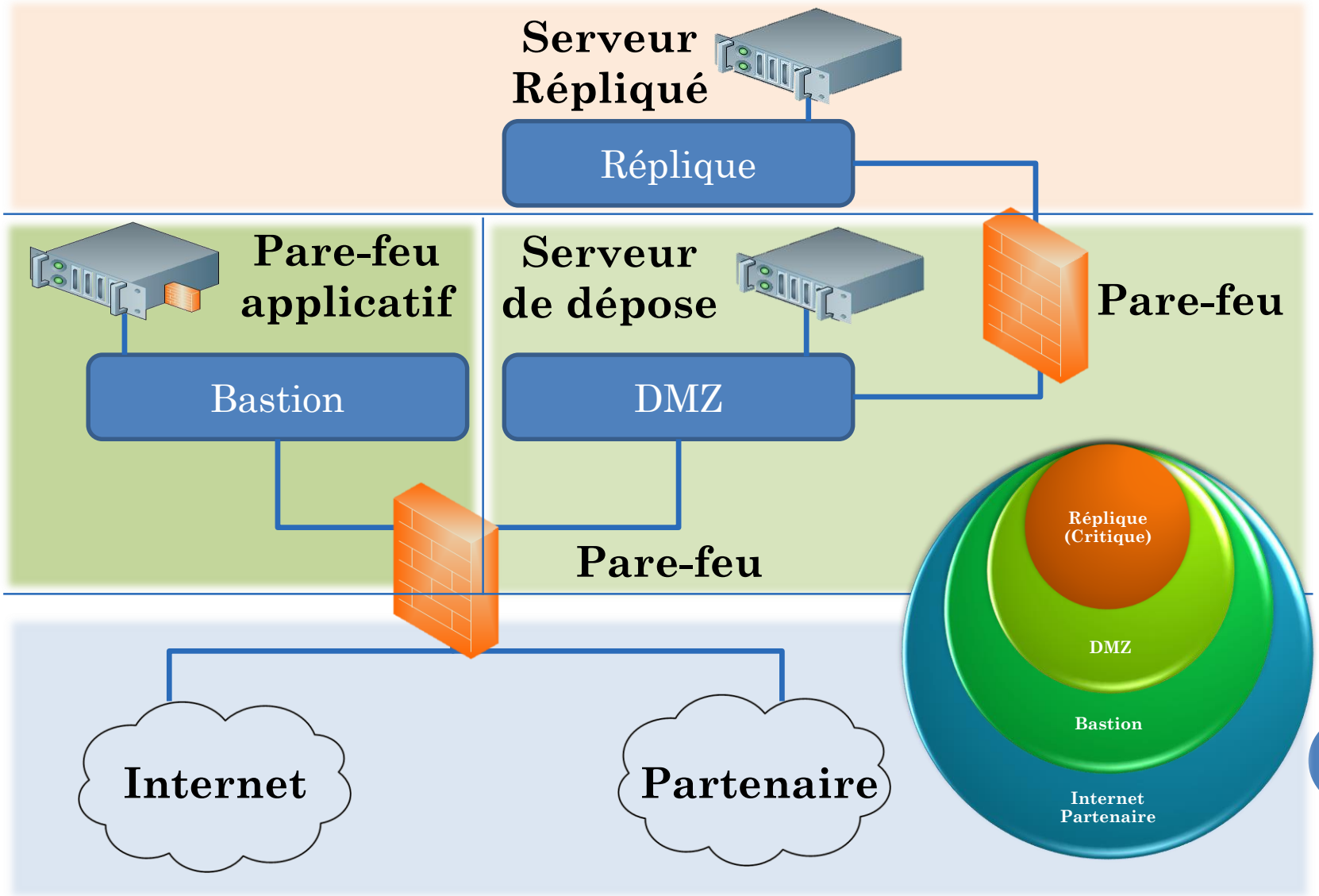
- Mise en place d'un serveur de plan de vol répliqué
- Création d'une zone spécifique pour le serveur répliqué (réplique)

Source / destination	Internet	Partenaire	Bastion	DMZ	Réplique
Internet					
Partenaire			✓		
Bastion	✓	✓		✓	
DMZ			✓		✓
Réplique					

V. Cas d'application
3. Réplication
Schéma



V. Cas d'application
3. Réplication
Schéma - zones



V. Cas d'application
4. Disponibilité
Besoins

Besoins :

- Offrir plus de disponibilité
- Optimiser la réponse à la charge vs consommation énergétique
- Accélérer la reprise d'activité
- Faciliter la maintenance
- Faciliter la mise en place d'évolutions

- Double source électrique (groupe électrogène, batterie)

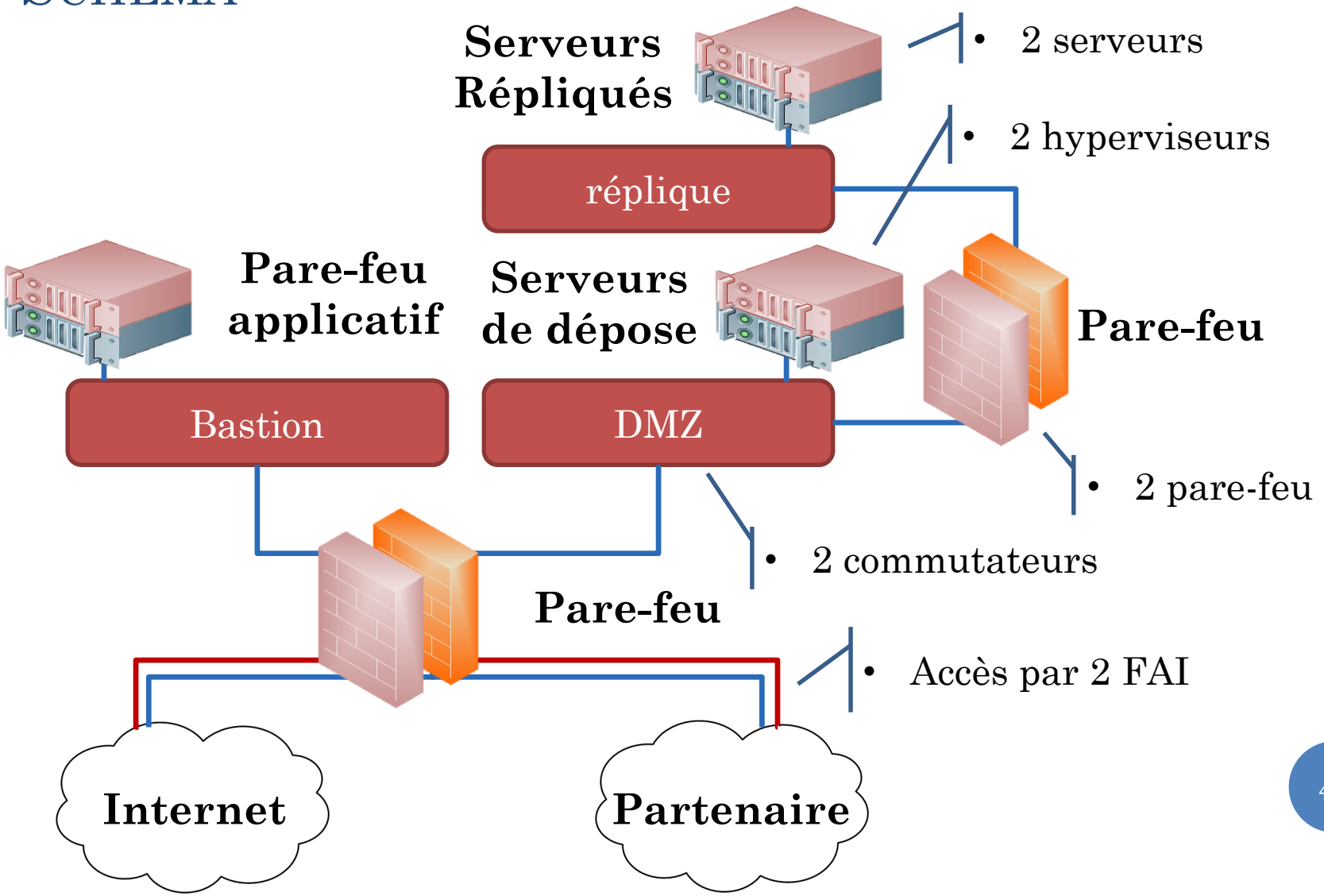
- Double accès Internet / partenaire par 2 FAI
- → Répartition de charge ou mise à jour du DNS

- Taux de service 99,99 % (~1 heure/an)
- → Remplacement à froid du matériel

- Taux de service 99,999% (~5 minutes/an)
- → Remplacement à chaud du matériel (doublement pare-feu, commutateurs, proxy, serveurs)

- Virtualisation des serveurs et / ou proxy (hyperviseurs)

V. Cas d'application
4. Disponibilité
Schéma

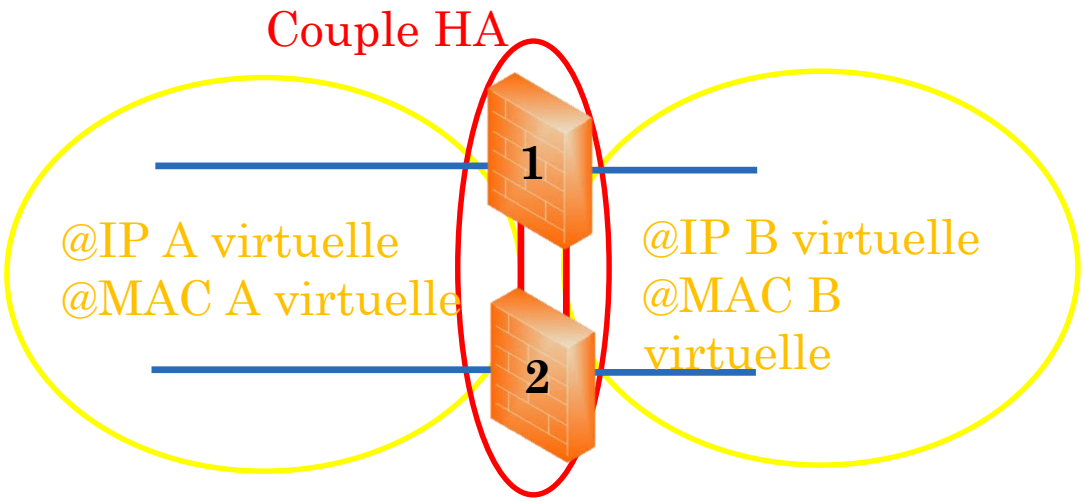


4. Disponibilité

Haute Disponibilité (HD) / High Availability (HA)

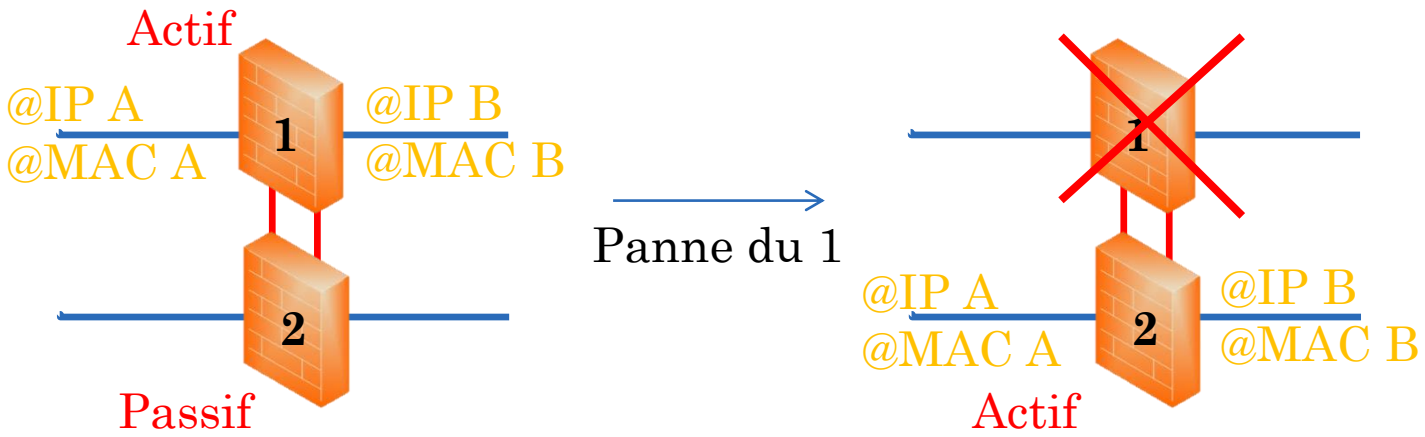
- Principaux modes HA :
  - **Actif / Passif** : Une seule machine transfère de la donnée à un instant donné dans le couple.
  - **Actif / Actif** :
    - Plusieurs machines actives à un instant donné.
    - Correspond à du loadbalancing.
  - Il existe plusieurs cas au-delà de 2 machines dans le cluster.

- Un couple HA utilise une @IP et une @MAC virtuelle
- Election distribuée de l'unité active
- Plusieurs protocoles : VRRP, HSRP, CARP, heartbeat et d'autres propriétaires
- Existe pour les pare-feu, proxys, serveurs



4. Disponibilité

Haute Disponibilité (HD) / High Availability (HA)

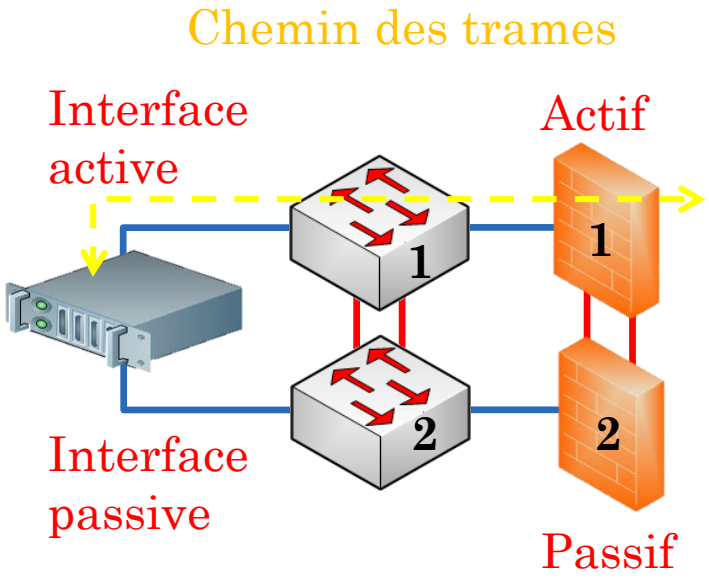


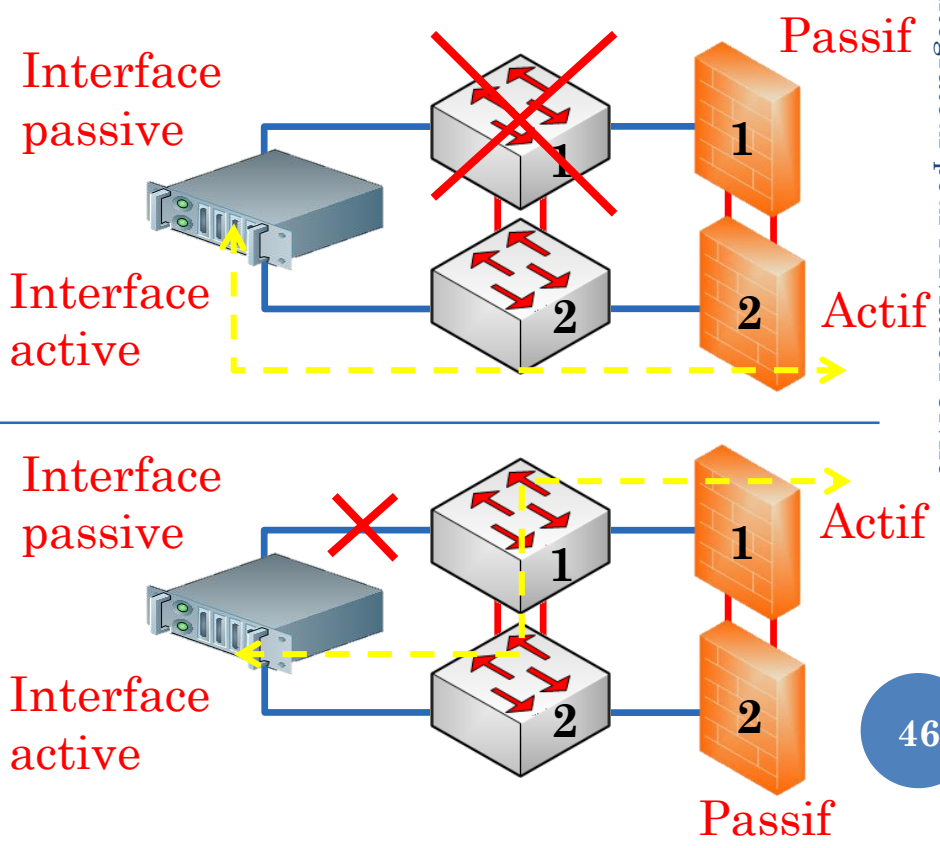
Split Brain

- Se caractérise par la présence sur le réseau de deux unités actives
- Deux @IP et @MAC sur le réseau au même moment, ça peut faire mal !!!
- → Attention à ne pas couper les liens HA (bien les identifier avant toute opération)
- → Il est conseillé d'avoir 2 liens HA
- Conseil : utilisé un câble d'une autre couleur

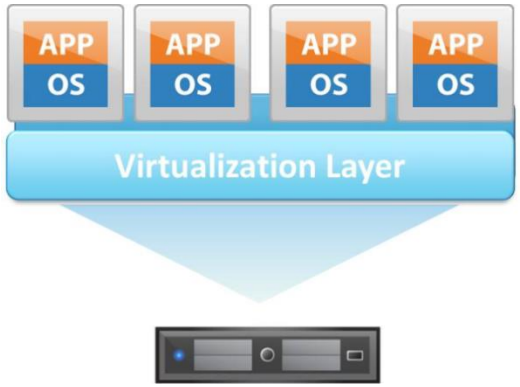
V. Cas d'application
4. Disponibilité
Double raccordement

- Haute disponibilité des commutateurs
  - Mise en pile : par câble spécial ou LACP (agrégation de liens)





V. Cas d'application
4. Disponibilité Virtualisation



Avantages

- Economique
- Modulaire
- Restauration simplifiée
  → Reprise d'activité rapide
- Evolutivité
- Allocation dynamique des ressources
- Certains produits uniquement virtualisés

Inconvénients

- Point de défaillance commun
  → Doubler les hyperviseurs
- Ajoute du code
  → Plus de vulnérabilités
- Matériel plus cher à l'achat
- Composant supplémentaire à administrer

V. Cas d'application
5. DoS
Besoins

Besoins :

- Se protéger du déni de service

- Virtualisation
- DNS balancing sur les différents FAI
- Bloquer au niveau des pare-feu frontaux
- → limiter une IP à un certain nombre de connexions
- → limiter le nombre de connexions semi-ouvertes
- Mise en cache au niveau des proxys
- Duplication de l'architecture sur un autre site

6. Détection d'intrusion

Besoins

Besoins :

- Détecter les comportements anormaux
- Se mettre en capacité de détecter une attaque
- Se mettre en capacité d'analyser une attaque à posteriori

- Supervision de l'architecture
- → Mise en place d'un serveur de supervision

- Récupération des logs des équipements
- → Synchronisation NTP pour la datation des logs

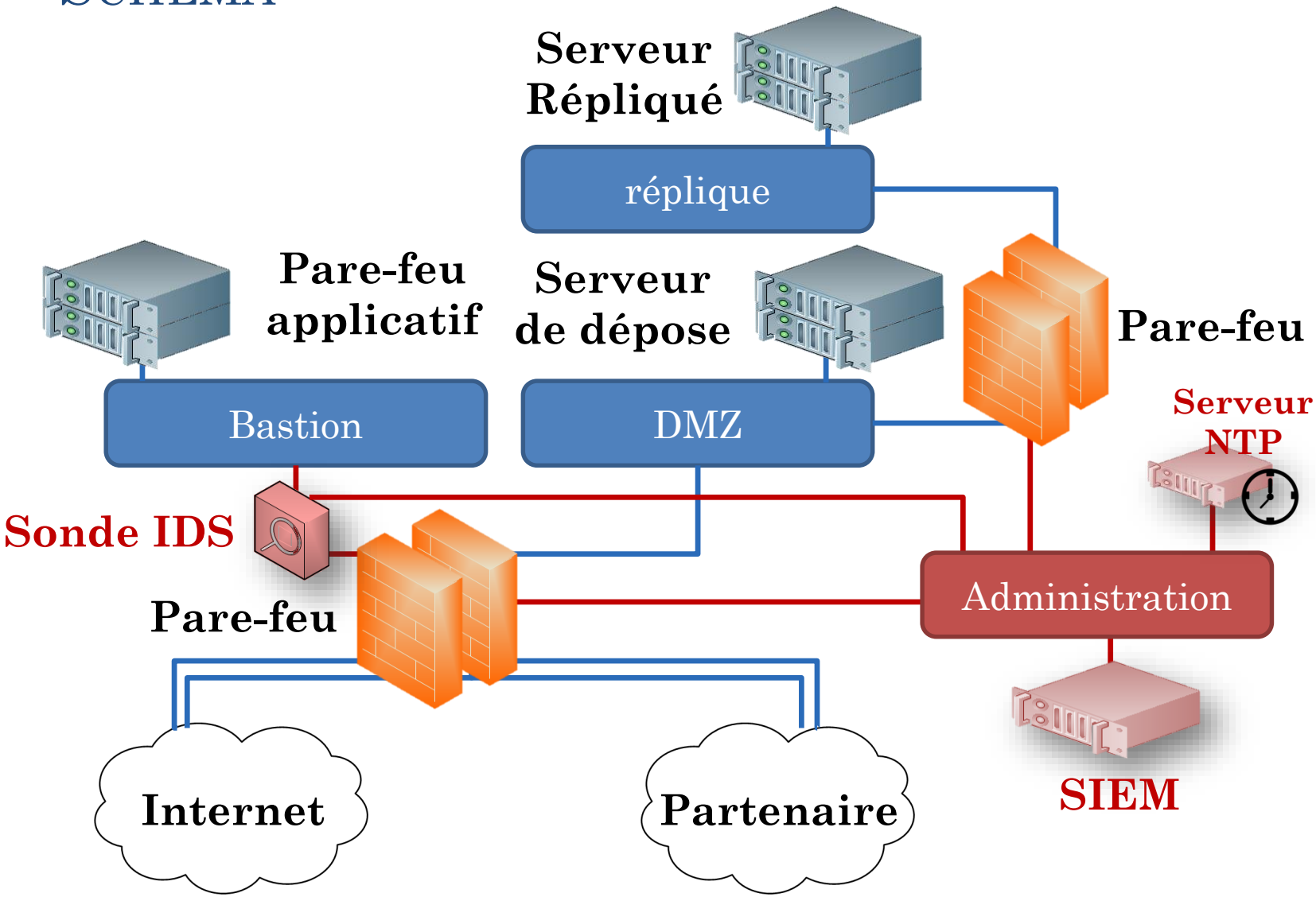
- Analyse et corrélation des logs

- Intrusion Detection System

- Vérification d'intégrité des systèmes (cf. durcissement système)

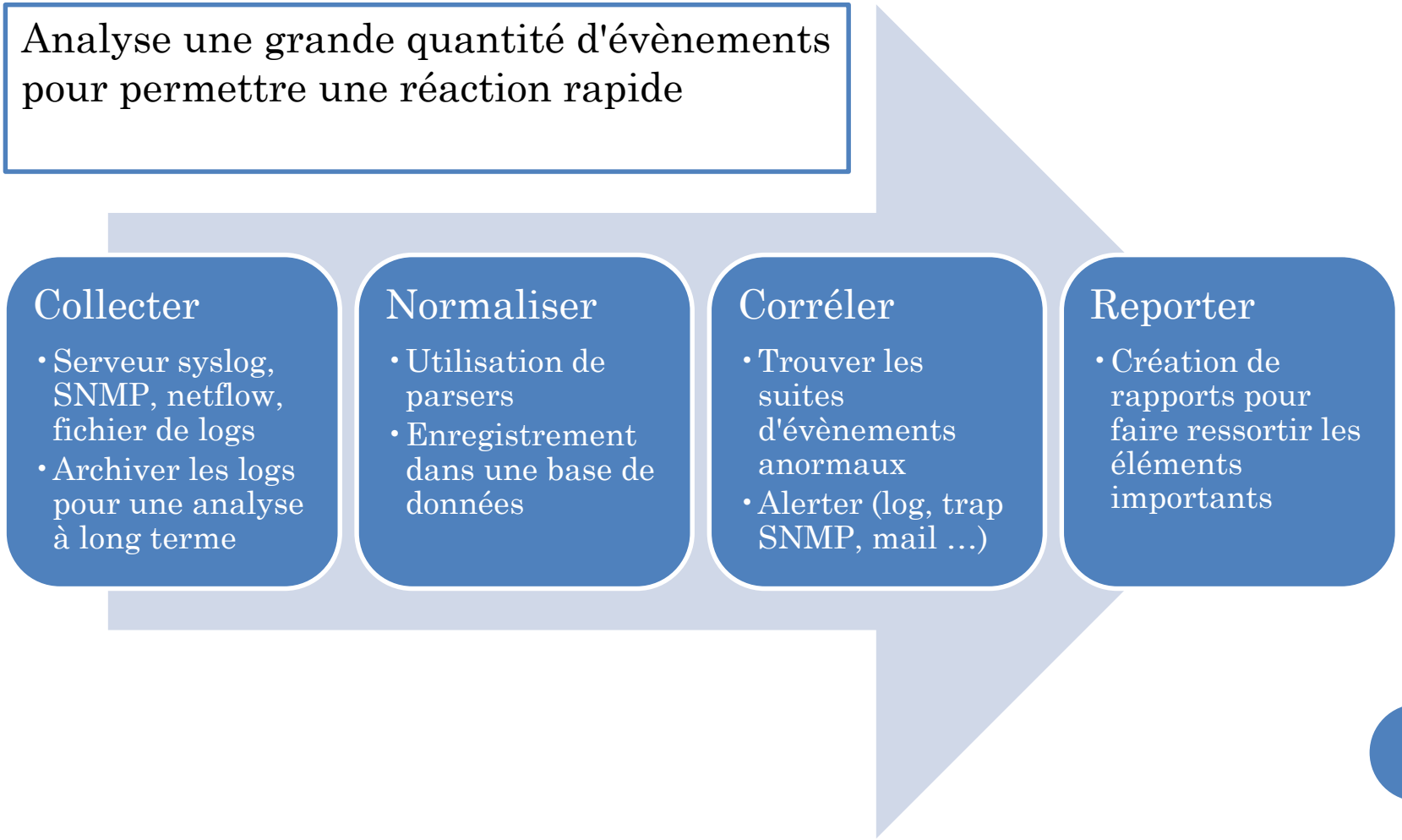
6. Détection d'intrusion

Schéma



V. Cas d'application
6. Détection d'intrusion
SIEM (Security Information Event Management)

Analyse une grande quantité d'évènements pour permettre une réaction rapide



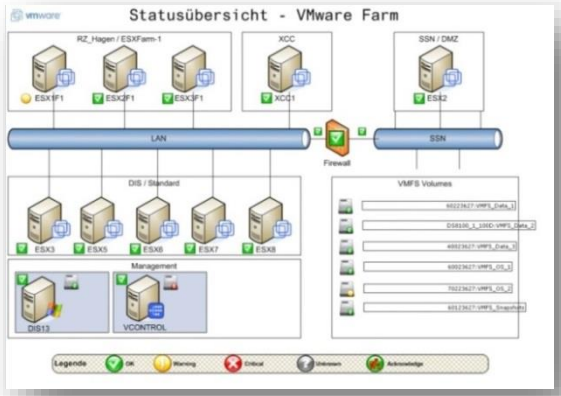
V. Cas d'application
6. Détection d'intrusion
Supervision

Objectifs

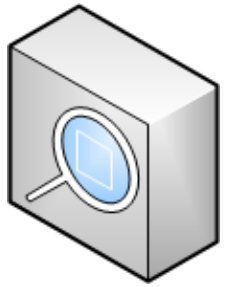
- Connaitre l'état de ses systèmes en "temps réel"

- A défaut d'empêcher une attaque, la détecter le plus vite possible
- Permet une analyse rapide de la situation
- Permet une reprise d'activité plus rapide

- Un protocole de prédilection : SNMP
  - SNMP v1 et v2 : nom de communauté en clair
  - **SNMP v3** : authenticité, confidentialité (AES128/DES) et intégrité (SHA1/MD5)
  - Communauté ou utilisateur en **lecture seule** ou lecture écriture (ro/rw)
- Pool (UDP/161) / Trap (UDP/162)
  - **Privilégier le pool** car assurance de connaitre l'état réel
  - Un trap peut se perdre ou peut ne pas être émis
- Exemple :
  - cas de panne électrique d'un équipement
    - pas de dernier souffle pour envoyer un trap
  - Trap au milieu d'une congestion
- Synoptiques



6. Détection d'intrusion IDS / IPS



Objectif

- Détecter les comportements suspects sur le réseau

- IDS : non bloquant
- IPS : bloquant (risqué en cas de faut positif)

- Plusieurs types :
  - NIDS (Network)
    - Dans les pare-feu
    - Appliance dédiée
  - HIDS (Host) : Directement sur un hôte

- Très consommateur en ressource (regex/contextes)
  - → Débit de traitement très limité (goulot d'étranglement)
- Demande beaucoup de temps de configuration (quasi permanent)
  - → Les seuils de détection doivent suivre l'évolution du trafic
- Pas très utile si personne n'analyse et n'est capable de réagir rapidement

V. Cas d'application
6. Détection d'intrusion
Deep Packet Inspection (DPI)

Objectif :

- Analyser le trafic en profondeur (conjointement avec IDS)
- Retracer un incident / attaque au niveau de plus bas
- DLP : Data Leak Prevention
- Par exemple capable de reconstruire une session de surf sur Internet

Prérequis :

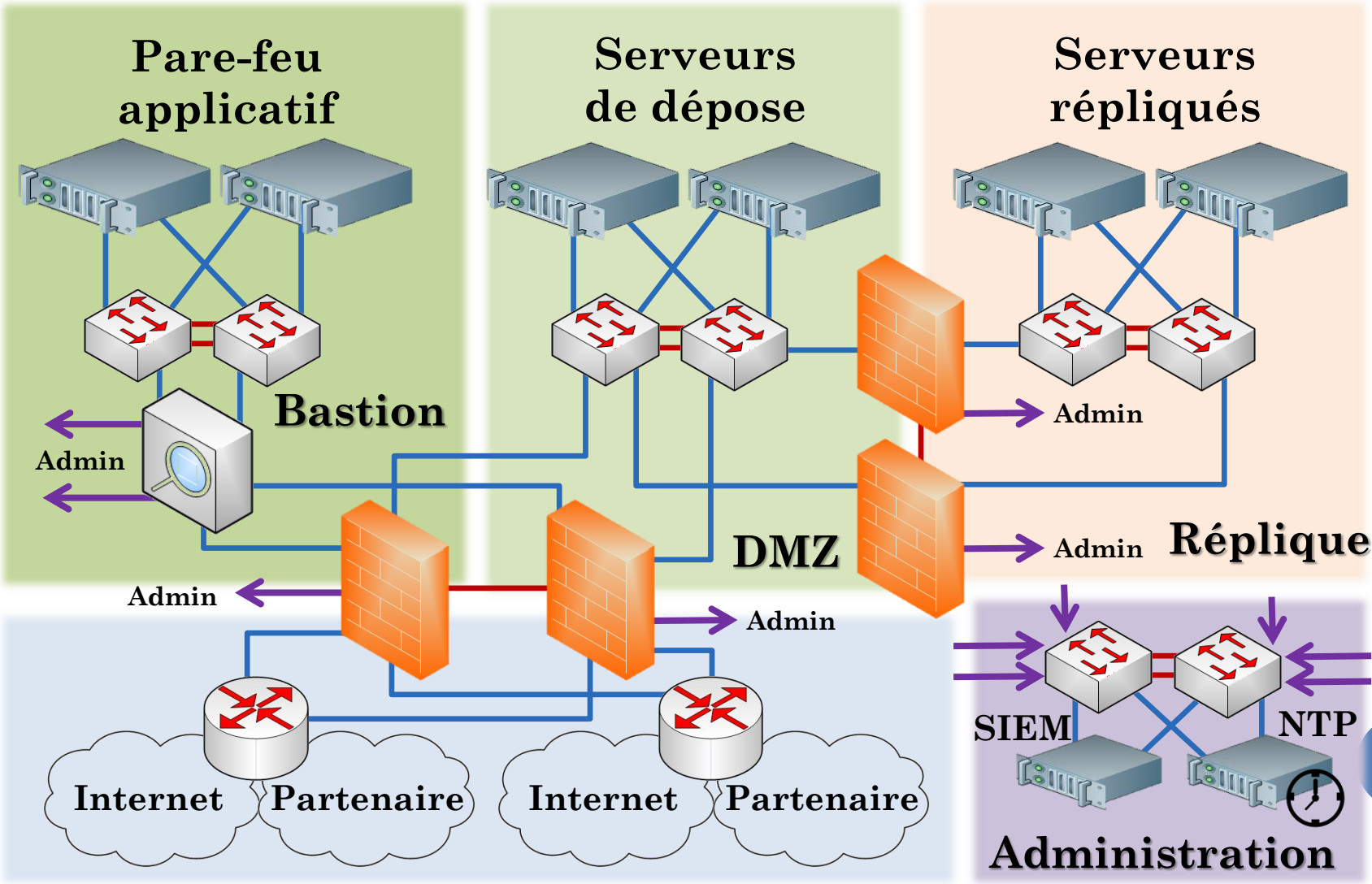
- Collecter toute l'information sur le réseau (capture réseau)
- → mirroring / SPAN port sur les commutateurs
- → TAP (Test Acces Port) : recopie du signal Ethernet
- Capacité de rétention importante (gourmand en ressources, x10 sur les logs)
- Sur dimensionner les liens

Limitations :

- Chiffrement (proxy SSL)
- DoS
- Faible temps de rétention (quelques jours) → l'attaque doit être détectée rapidement
- Stéganographie

- Vie privée : Collecte de masse ≠ surveillance de masse

V. Cas d'application
Schéma physique global



Plan

I. Présentation
II. Contexte / Enjeux
III. Aspects réglementaires
IV. Architecture réseau
V. Cas d'application
VI. **Durcissement système**
VII. Intégration système
VIII. Cadre organisationnel
IX. Conclusion

VI. Durcissement système
Techniques de base

- Ensemble de techniques qui visent à rendre un système plus résistant aux attaques et qui le place dans les meilleures conditions pour assurer sa mission avec la meilleure disponibilité possible

- Réduction de la surface d'attaque

- Inclure dans le système uniquement ce qui est nécessaire (uniquement le code nécessaire pour rendre le service attendu)
- Tout code est potentiellement vecteur de faille
- Principe du "présent uniquement si nécessaire"

- Limiter les droits des utilisateurs :
  - privation de shell
  - droits sur l'arborescence (/var/log, /etc, /root, /bin, /sbin, /usr …)
  - Appartient à des groupes limités en droit

VI. Durcissement système
Techniques liées aux utilisateurs

- Complexité minimale sur les mots de passe (cracklib : complexité et dictionnaire)
- Durée de vie définie pour les mots de passe

- Limiter le nombre d'utilisateurs au strict nécessaire

- Dédier un utilisateur système pour chaque service
- Limiter les droits donnés aux programmes (en les exécutant avec un utilisateur bridé)

- Limiter le recours à l'utilisateur root
- Interdire les connexions directes par l'utilisateur root (login prévisible)

Bonnes pratiques

- Favoriser des méthodes d'authentification multi-facteur
- Ne pas autoriser les utilisateurs "groupe"

VI. Durcissement système
Techniques liées aux services

- Limiter les accès externes à quelques services et quelques utilisateurs aux droits limités
- Mettre en place du bannissement en cas d'échecs de connexion répétés

- Limiter les services qui s'exécutent

- Limiter les services accessibles de l'extérieur / de l'intérieur (nmap/netstat)
- Réduire la surface d'attaque réseau

- Limiter les informations sur la version et le programme qui rend le service (mode production)

- Limiter les services trop bavards (il suffit de regarder ce qui sort d'une machine)
- Exemple : MaJ, rapport de crash, découverte réseau (Avahi), Netbios/SMB …

- Limiter la dérive système, l'accumulation non maitrisée (quota, rotation, purge)
- Exemple : logrotate, coredump, /home, /var/www …

- Durcir les couches réseau (TCP Wrapper, ARP statiques, routage statique, DNS, réponses ICMP)
- Configurer les options systèmes (syscontrol)

VI. Durcissement système
Intégrité

Objectif :

- Détecter les modifications apportées à un système
- Détecter les intrusions en analysant régulièrement l'intégralité du système
- Garantir l'intégrité du système (garantie d'assez bas niveau)

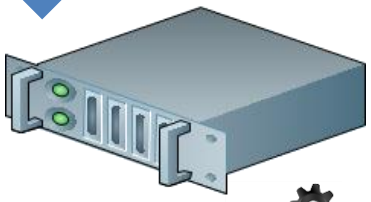
Paramètres enregistrés :

- Somme de contrôle
- Droits
- Dates (création, dernier accès, dernière modification)
- Inode
- Nombre de fichiers
- …

VI. Durcissement système
Intégrité - fonctionnement

1
- Un fichier de référence est généré à l'installation (quand le système est considéré comme intègre)
- Il est sauvegardé dans un lieu sûr pour analyse post mortem
- Certains logiciels fournissent des signatures de fichiers bien connus

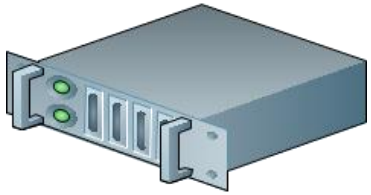
2
- Une analyse est effectuée régulièrement pour analyser les éventuelles modifications
- En cas de modification justifiée, la nouvelle base est considérée comme nouvelle base de référence



1

Vérification d'intégrité

Base de référence



2

Base issue de
l'analyse du système

Plan

I. Présentation
II. Contexte / Enjeux
III. Aspects réglementaires
IV. Architecture réseau
V. Cas d'application
VI. Durcissement système
VII. **Intégration système**
VIII. Cadre organisationnel
IX. Conclusion

VII. Intégration système
Principes de base

Objectifs :

- Automatiser pour éviter les erreurs
- Accélérer la reprise d'activité
- Protéger l'utilisateur de sa méconnaissance en le guidant
- Uniformiser les systèmes pour rendre la maintenance plus aisée

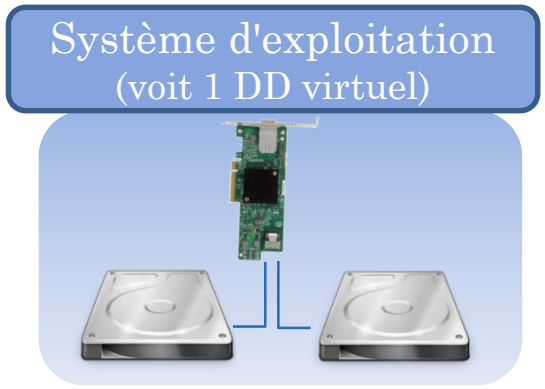
- Toujours garder en tête le fragile équilibre : sécurité / fonctionnalité / facilité d'utilisation
- Le bon système pour les bons besoins
- Automatisation de l'installation :
  - Outil : Preseed (Debian, Mint, Ubuntu …) kickstart (RedHat, Fedora, CentOS …)
  - Formatage
  - Configuration réseau
  - Sélection des paquets (apt/rpm/ports/…)
  - … tout ce qui est demandé lors d'une installation classique
  - **Durcissement** (scripts)
  - Personnalisation de l'environnement (scripts)
  - Configuration de l'accès d'administration
  - Configuration des services
  - Création des utilisateurs
  - Modifications des mots de passe (TOUS, on ne laisse pas de mot de passe par défaut)

VII. Intégration système Disponibilité

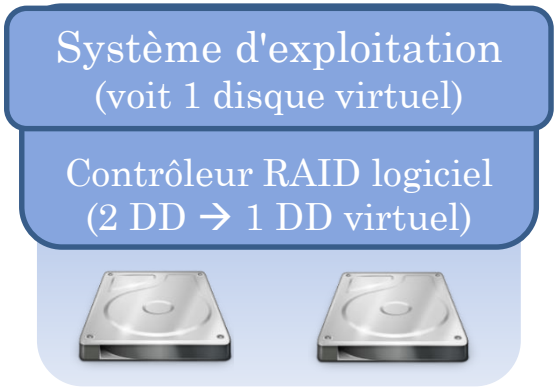
Disponibilité système :

- Dupliquer la donnée :
  - système de fichier réparti
  - base de données répartie
- Mise en HA : HeartBeat (HB)
  - Partage d'adresse similaire au VRRP
- Superserveurs : relance un service en cas de problème (xinetd)
- RAID : tolérer des pannes sans perte de données

RAID



RAID software



VII. Intégration système DEBIAN

debian

- Paquets précompilés (système APT)
- Communauté très développée
- MaJ fréquentes
- Relativement sécurisé / stable
- Pérennité du projet
- LTS (Long Term Support)

- Ne sacrifie pas l'évolutivité pour la sécurité
- Très répandu
- Encore plus répandu par héritage (Ubuntu, Mint, Kali, DVL …)
- Pas de support commercial, contrairement à RedHat

VII. Intégration système
Système de dépôts (APT)

- Plein de miroirs (pas forcément sous l'autorité de la communauté)
- Garantie sur l'origine du paquet (signature numérique)

- Clé publique officielle de la version livrée dans le CD d'installation (apt-key dans **trusted.gpg**)
- Signature du fichier release : http://ftp.fr.debian.org/debian/dists/wheezy/**Release.gpg**
- Descriptif des fichiers du dépôt (index) : http://ftp.fr.debian.org/debian/dists/wheezy/**Release**
  - Contient le haché de tous les fichiers du dépôt : MD5, SHA1, SHA256
  - On peut avoir confiance dans le contenu des infos des fichiers du dépôt par vérification du hash

Fichier "Release"

- Origin: Debian
- …
- Version: 7.9
- Codename: wheezy
- Date: Sat, 05 Sep 2015 11:44:23 UTC
- Architectures: amd64 armel armhf i386 ia64 kfreebsd-amd64 kfreebsd-i386 mips mipsel powerpc s390 s390x sparc
- Components: main contrib non-free
- Description: Debian 7.9
- Released 05 September 2015
- MD5Sum:
  - **e28e71c16cac0c411bf5b2e461dff972 304063644 Contents-amd64**
  - **ea4195b21ab485e59b9ef30357e709ca 21606550 Contents-amd64.gz**
  - …

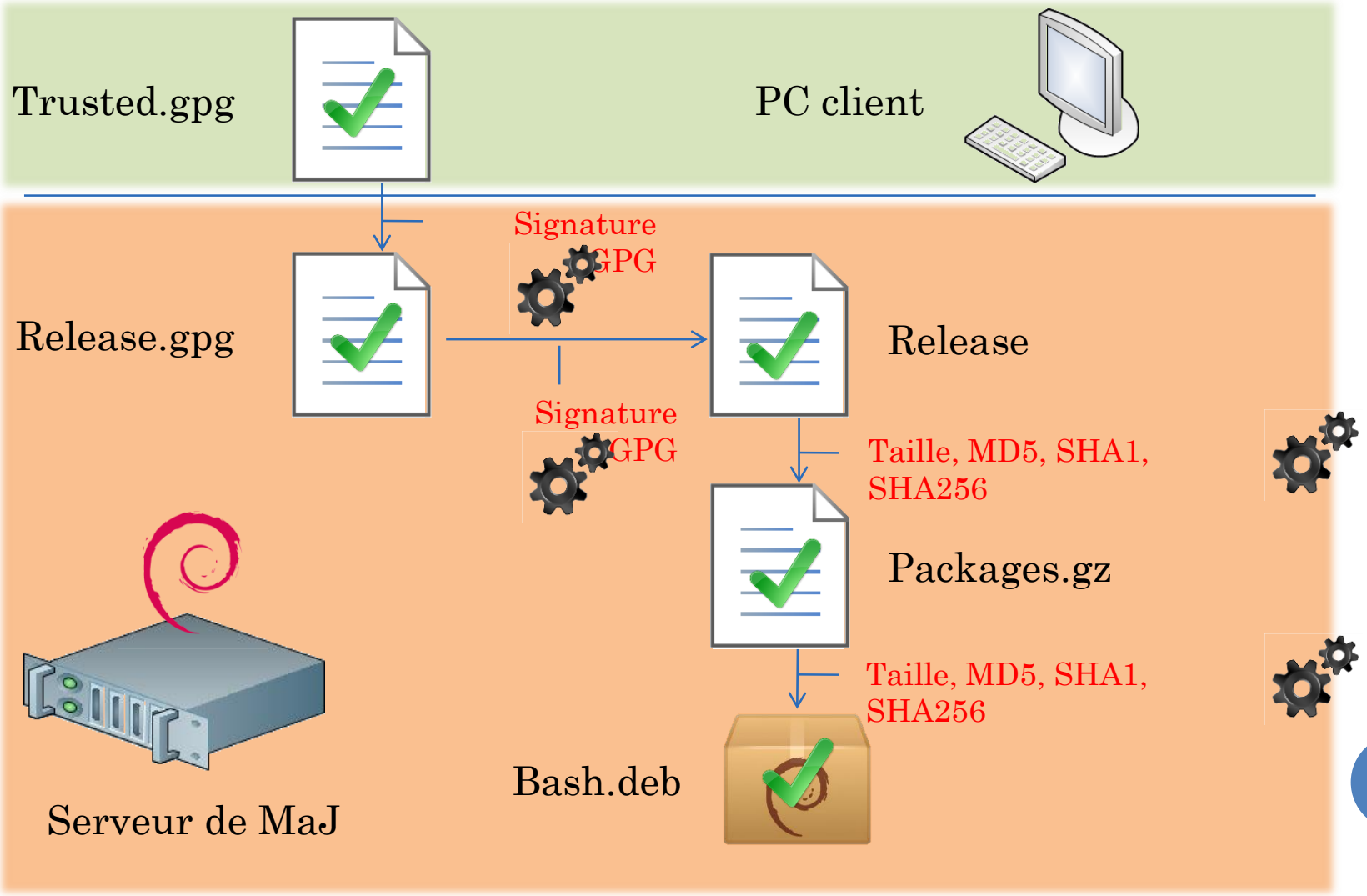
VII. Intégration système
Système de dépôts (APT)

- Toutes les propriétés des paquets sont dans : http://ftp.fr.debian.org/debian/dists/wheezy/main/binary-i386/Packages.gz
  - on peut avoir confiance dans le contenu des paquets après vérification des propriétés (nom, taille, hachés)

Exemple : Bash

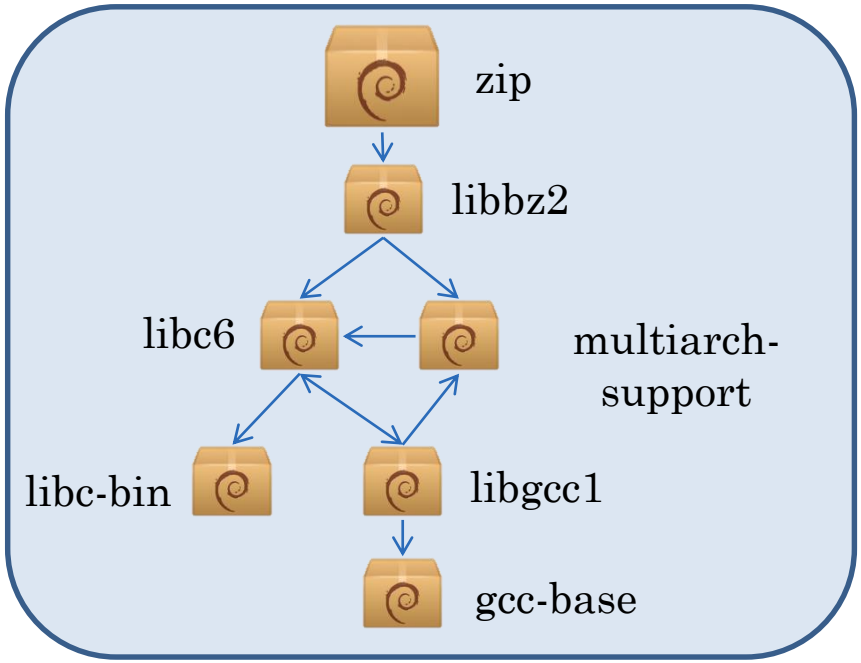
- Package: bash
- Version: 4.2+dfsg-0.1+deb7u3
- Installed-Size: 3902
- Maintainer: Matthias Klose doko@debian.org
- Architecture: i386
- Replaces: bash-completion (<< 20060301-0), bash-doc (<= 2.05-1)
- **Depends: base-files (>= 2.1.12), debianutils (>= 2.15)**
- Pre-Depends: dash (>= 0.5.5.1-2.2), libc6 (>= 2.11), libtinfo5
- Recommends: bash-completion (>= 20060301-0)
- Suggests: bash-doc
- Conflicts: bash-completion (<< 20060301-0)
- Description: GNU Bourne Again Shell
- […]
- **Filename: pool/main/b/bash/bash_4.2+dfsg-0.1+deb7u3_i386.deb**
- **Size: 1472464**
- **MD5sum: 0fd27715e269feda81dcd59fb79665f1**
- **SHA1: 68d4446dc31c4fc1555d6f6d432f2ccd31ffda4e**
- **SHA256: e69d34a618a00ec21b64c361eec491cb034336ca790668a42409ee39bf96ff78**

VII. Intégration système
Système de dépôts (APT)



VII. Intégration système
Système de dépôts (APT)

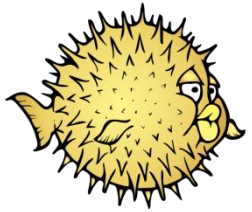
- Paquets : fichier ".deb" (tar.gz le plus souvent)
- Contient :
  - Binaires
  - Sources
  - Pages man
  - Fichiers de configuration
  - …



- Arbre de dépendances
  - Exemple : **zip**
  - ATP abstrait la complexité
    - apt-get install zip

- Intégrité du contenu du CD (paquets .deb en grande partie)
  - md5 de tous les fichiers du CD
  - Auto-vérification du média d'installation

VII. Intégration système OpenBSD

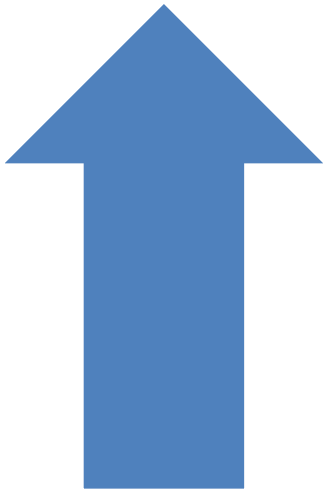


OpenBSD

- Philosophie : Sécurisé par défaut

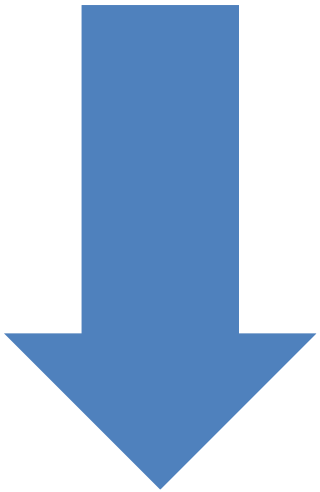
• Durcissement fait • Facilite l'intégration • Très utilisé pour les systèmes sécurisés • Paquets précompilés (système de port)	• Austère • Maj de sécurité requièrent recompilation du système (long et interruption de service)

VII. Intégration système Diversité



Avantages

- Favoriser la diversité pour éviter les SPoF
- Requiert des connaissance mutli-système pour parvenir à mener une attaque complète
- L'un des seuls remède efficace aux zeroday



Inconvénients

- Il n'y a qu'un ensemble fini de systèmes
- Pas de capitalisation
- Nécessite plus de ressources :
  - Un effort de formation
  - Un effort de maintenance
  - Un effort pour l'évolution

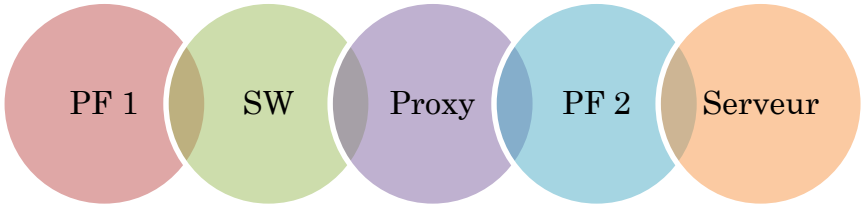
Plan

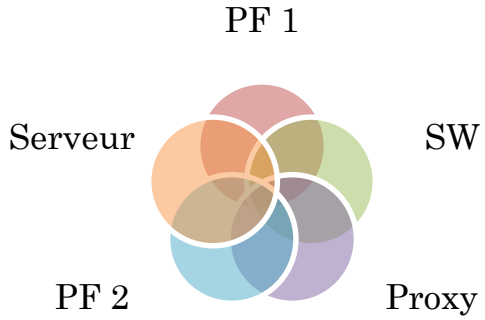
I. Présentation
II. Contexte / Enjeux
III. Aspects réglementaires
IV. Architecture réseau
V. Cas d'application
VI. Durcissement système
VII. Intégration système
VIII. **Cadre organisationnel**
IX. Conclusion

VIII. Cadre organisationnel
Gestion des vulnérabilités

1. Vérifier si les systèmes possèdent des vulnérabilités connues
   - Détecter les versions des systèmes par scan (actif/passif) ou inventaire
   - S'appuyer sur les bases de connaissance de vulnérabilité
     - CVE : Common Vulnerabilities et Exposures
     - CERT : Computer Emergency Response Team

2. Vérifier si l'ensemble des vulnérabilités expose à un risque





3. Patcher les systèmes pour éliminer le risque lié à la vulnérabilité

❖ <u>Limitation</u> : ne protège pas des vulnérabilités non connues

VIII. Cadre organisationnel
AUDIT

- Audit : Vérifier la conformité du SI à une référence

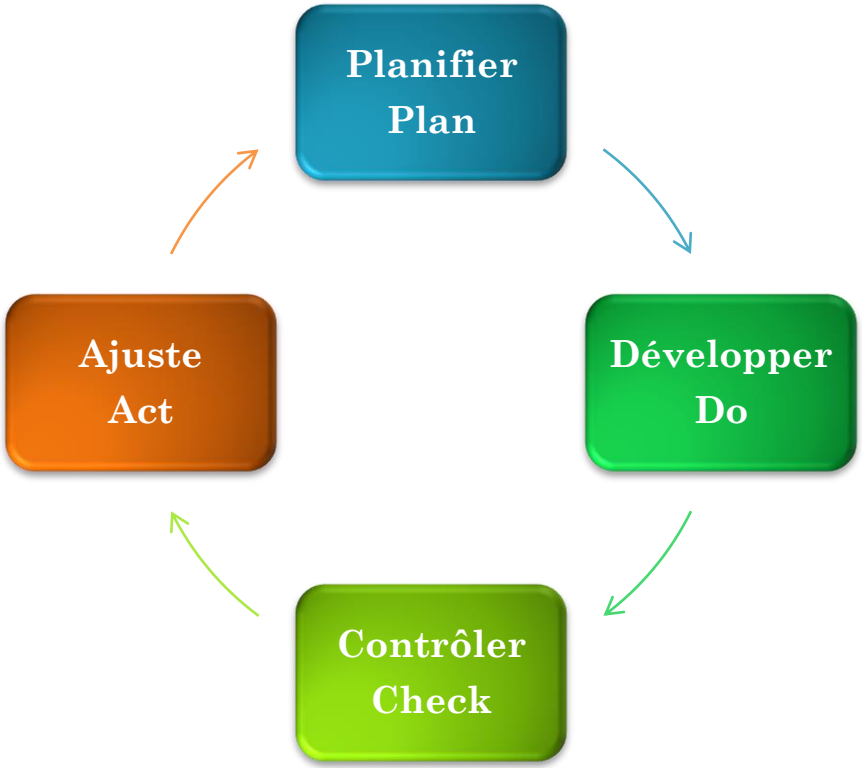
- Audit organisationnel : regarde la cohérence avec des normes (ISO 2700X, PCI-DSS…)
- Audit technique : test de pénétration (pentest : vérifier les mécanismes de sécurité en se mettant à la place d'un attaquant)

- évalue la non-conformité, identifie des risques (outils : EBIOS, MARION, MEHARI …)

- Termine la roue de Deming (ISO 2700X)
  - principe d'amélioration continue

VIII. Cadre organisationnel Audit et SMSI

- SMSI : Système de Management de la Sécurité de l'Information
- Principe d'amélioration continu (PDCA / PDSA)
- Défini dans la norme ISO 27001



Plan

I. Présentation
II. Contexte / Enjeux
III. Aspects réglementaires
IV. Architecture réseau
V. Cas d'application
VI. Durcissement système
VII. Intégration système
VIII. Cadre organisationnel
IX. **Conclusion**

IX. Conclusion
Cycle de vie d'une architecture sécurisée

Avant l'attaque

- Architecture : on construit sa défense, on se prépare à subir une attaque (durcissement, réplication …)
- Procédures : isolation, bannissement, PRA : Plan de Reprise d'Activité / DRP : Disaster Recovery Plan …

Pendant l'attaque

- Détecter l'intrusion (supervision, logs, intégrité, IDS)
- Limiter les impacts

Après l'attaque

- Avoir les moyens de retrouver l'attaquant (logs, intégrité, DPI, inforensic)
- La vie continue, il faut reprendre l'activité rapidement
- Reconstruire une défense solide face à l'attaque menée et à ses variantes

IX. Conclusion
Conseils

Conception

- Une attaque profite des cas limites non prévus ! (DoS, buffer overflow)
- → toujours voir le pire et le mal partout
- → la paranoïa est "saine" en sécurité
- Ne pas mettre d'œillères, toujours imaginer tous les cas d'attaque possibles

- Toujours garder en tête l'équilibre : sécurité/fonctionnalité/facilité d'utilisation
- La sécurité n'est jamais une fin en elle-même, elle n'est utile qu'à protéger ce qui a réellement de l'importance

Support

- En réseau, vérifier couche par couche (OSI)
- En système, ça n'est pas aussi simple, approche en couche moins évidente
  - PEBCAK : Problem Exists Between Chair And Keyboard
  - N'est pas la réponse à tout problème, mais en explique beaucoup

IX. Conclusion
En résumé

Ingénieur sécurité vs Hacker

- L'ingénieur perd toujours, car il a plus à perdre (de l'argent, des vies, une image)
- Il est plus facile de détruire que de reconstruire
- On peut seulement se préparer au mieux pour affronter une attaque

"There is no patch to human stupidity"

- Unique vaccin : formation contre l'ingénierie sociale
- L'ingénierie sociale est souvent plus simple que de s'attaquer au technique

Réseau vs Sécurité

- En interconnectant on prend toujours un risque, il s'agit de le réduire au minimum
- Après il faut l'accepter (RSSI ou PDG), à défaut vivre avec

Merci pour votre attention

Contact

- aurelien.bouzon@alumni.enseeiht.fr