Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE LA DÉFENSE

Architectures multiniveau

Postes clients multiniveau et systèmes d'interconnexion

10/06/2008

DGA

DÉLÉGATION GÉNÉRALE POUR L'ARMEMENT

Contact:
CELAR/SSI/SSY/EA
Sébastien Gay

Les besoins multiniveau

- Mutualisation des moyens (poste de travail, réseaux)
  - ➔Amélioration de l'ergonomie,
  - ➔Réduction des coûts,
- Echanges interniveaux : interconnexions avec contrôle des flux et des données.
  - ➔Amélioration de l'efficacité

➔Dans les deux cas: Lutte contre les comportements à risque

Une contrainte sécuritaire

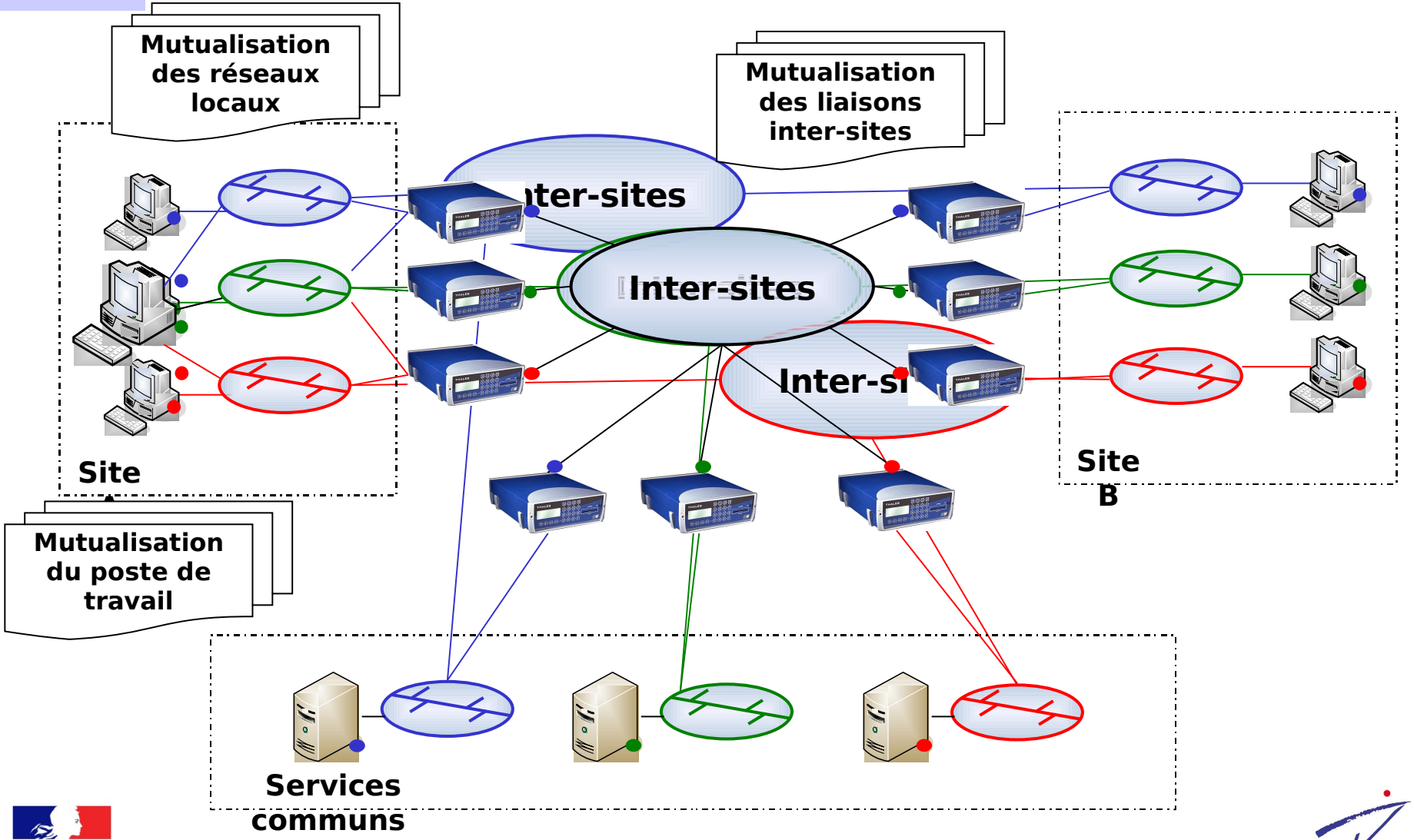
- Maintenir le cloisonnement entre les niveaux :
  - pour éviter la fuite d'informations d'un niveau haut vers un niveau bas (CONFIDENTIALITE)
  - pour éviter la corruption d'un niveau haut par des informations ou programmes d'un niveau bas (INTEGRITE et DISPONIBILITE)

Déclinée en contraintes techniques

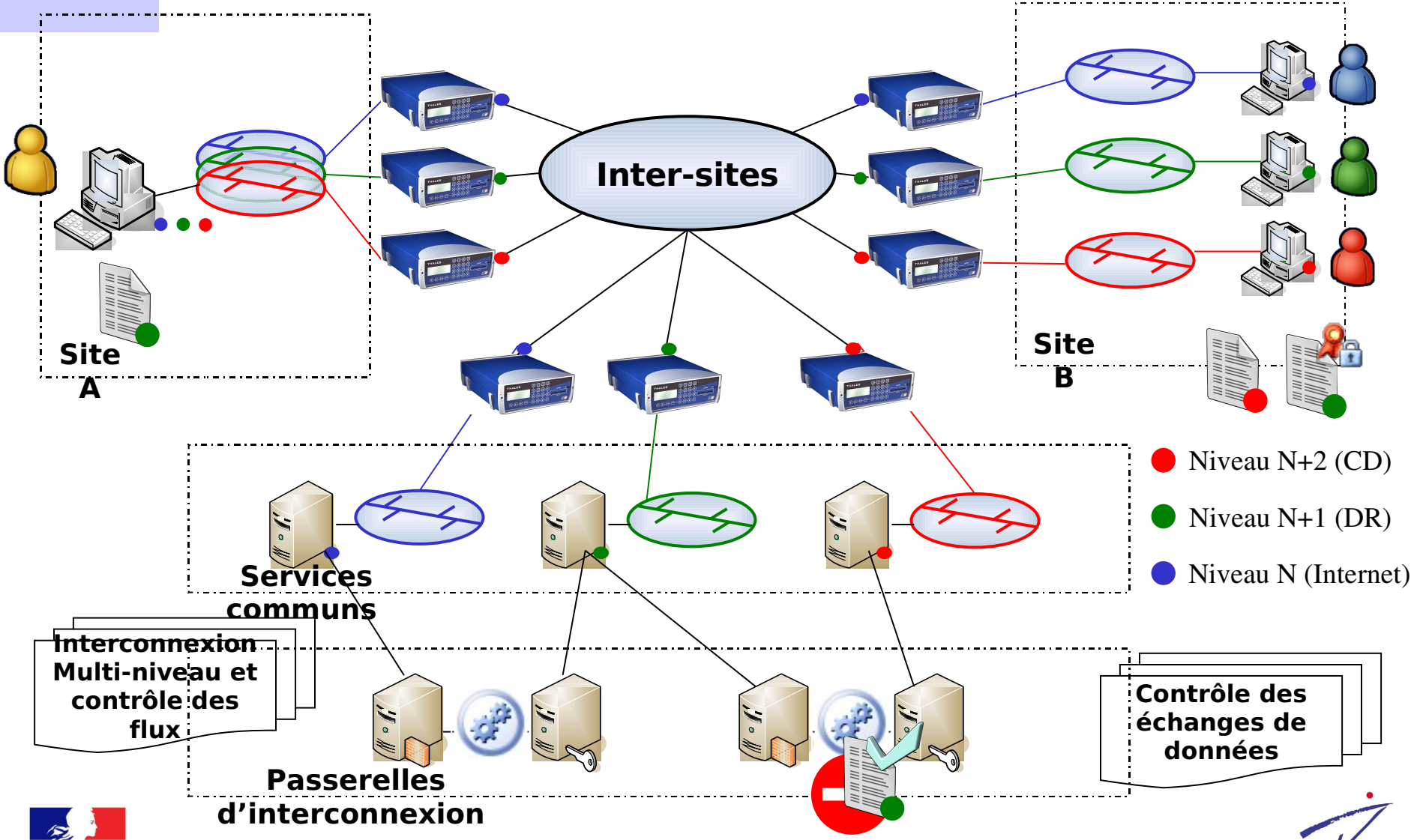
- Le cloisonnement doit être assuré à tous les niveaux (du matériel à l'information):
  - mémoire, disques durs, périphériques (y compris les écrans, claviers)
  - flux réseaux
- Tout en permettant des échanges contrôlés

⇨ Peut sembler contradictoire…

La mutualisation des moyens

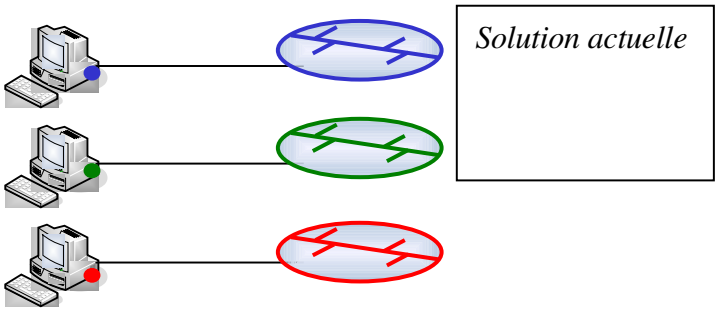


Les échanges inter-niveaux

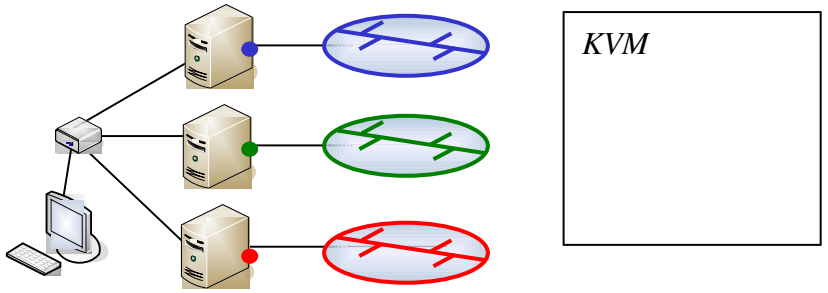


Poste multiniveau

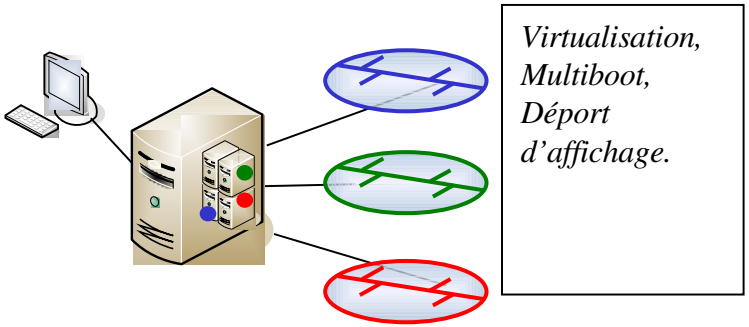
⇨ Typologie des solutions



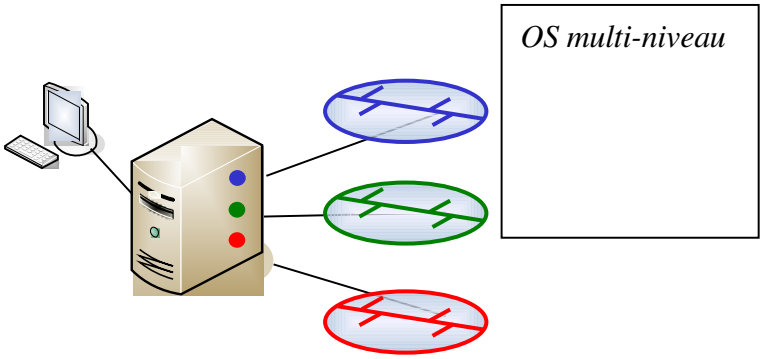
1. Pas de mutualisation



2. Mutualisation des périphériques



3. Mutualisation du hardware



4. Mutualisation de l'OS

Poste multiniveau

⇨ Distinction solutions alternées/simultanées

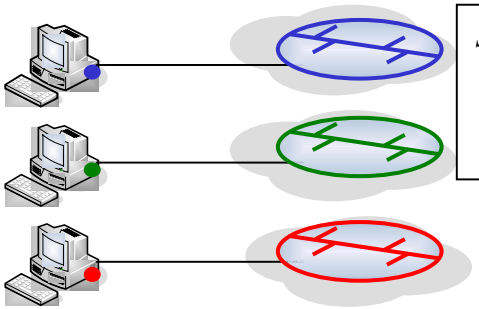
- Solutions alternées:
  - Nécessite un reboot pour changer de niveau
  - Exemples:
    - Commutation mécanique
    - Cloisonnement crypto des disques
    - Déport de disques sur le réseau (iSCSI, AoE)
- Solutions simultanées:
  - Permet un accès à tous les niveaux avec commutation « immédiate », sans reboot
  - Exemples:
    - Virtualisation
    - Cloisonnement
    - Déport d'affichage

Poste multiniveau
⇨ Axes d'étude

- Solutions alternées, KVM :
  - Zones mémoires des périphériques
  - Mémoire rémanente sur le poste
- Virtualisation
  - Sécurisation & test d'un virtualiseur
  - Définition d'une zone de confiance minimale pour l'implémentation de fonctions de sécurité
- Sécurité matérielle
  - Problème de maîtrise des plateformes matérielles (mécanismes de sécurité ou même fonctions standards)

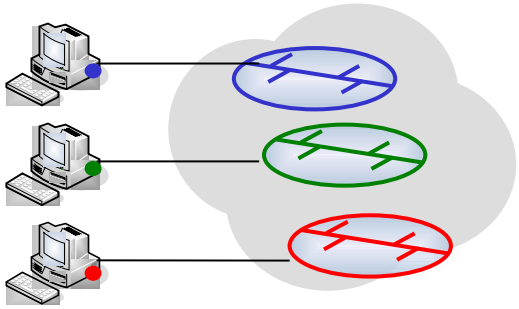
Cloisonnement de flux

⇨ Typologie des solutions



Solution actuelle

1. Réseaux physiques dédiés

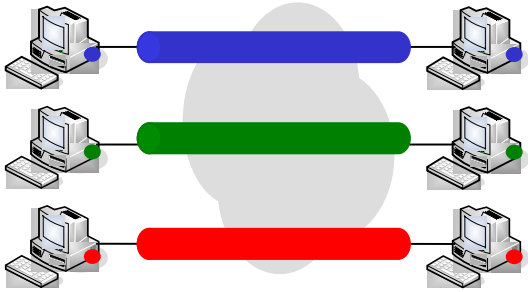


VLAN par port

VLAN avec authentification IEEE 802.1x

Marquage IEEE 802.1q interne ou externe

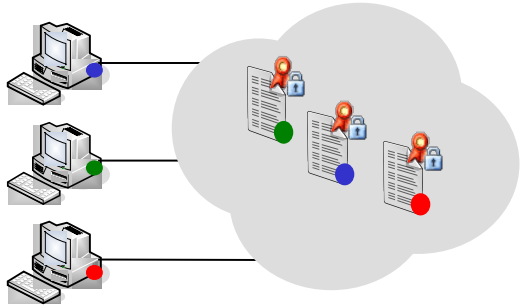
2. Réseaux virtuels de VLAN



Chiffreur externe mono ou multiniveau

Chiffrement IPsec (interne)

3. Réseaux virtuels VPN



Marquage des flux ou des données

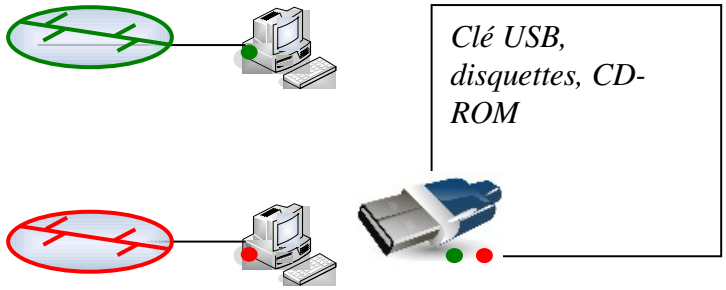
4. Réseau unique

Cloisonnement de flux
⇨ Axes d'étude

- VLAN
  - Problématique du marquage de confiance
- VPN
  - Problématiques de chiffrement multiniveau
  - Multiplication des tunnels
    - Problèmes flagrants d'administration
    - Mécanismes de mise en place automatique de tunnels (IPsec Discovery)

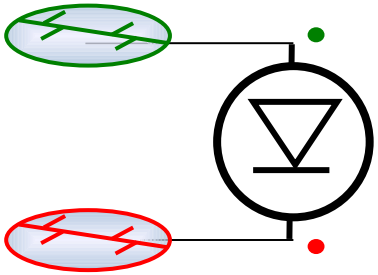
Echanges interniveaux

⇨ Typologie des solutions



Clé USB, disquettes, CD-ROM

1. Echanges hors-ligne

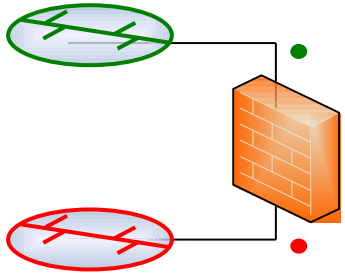


Diode

Sas de dépollution

Antivirus

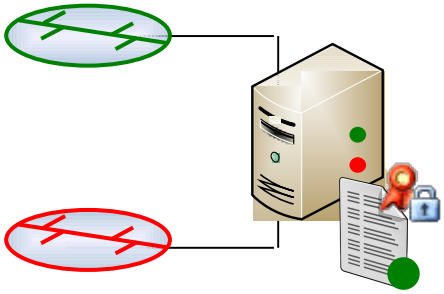
2. Echanges unidirectionnels



DMZ

Avec Pare-feu, proxy applicatifs

3. Echanges bidirectionnels avec contrôle des flux



Labellisation

4. Echanges de données bidirectionnels maîtrisés

Echanges interniveaux

⇨ Axes d'étude

- Dépollution
  - Filtrage/blocage de certains formats jugés dangereux
- Labellisation
  - Moyen technique de responsabilisation d'un utilisateur
  - Visionnage de confiance
    - Comment s'assurer que ce que signe un utilisateur est fiable?
  - Automatisation des échanges et problèmes de fusion
    - Comment déterminer à coup sûr de manière automatique le niveau des informations à exporter?
      - Sources et niveaux de sécurités divers en entrée
      - Traitements internes à l'application souvent compliqués (fusion de données)