



Dispositif DESIIR

Dispositif d'Echange Sécurisé d'Informations sans Interconnexion Réseau

EDF R&D

Arnaud TARRAGO, Pascal SITBON, Pierre NGUYEN

DESIIR@edf.fr



Besoins

- ✿ **Besoin d'une forte sécurité** (« sécurité physique », gestion de contenu)
 - Protection forte contre l'intrusion sur la zone de haute sécurité y compris en cas de vulnérabilités logicielles ou d'erreur de configuration
 - Protection contre les fichiers mal formés et les auto-exécutables

- ✿ **Besoin de fiabilité** (garantie de transfert, retransmission automatique)
 - L'émetteur doit savoir si son transfert a fonctionné

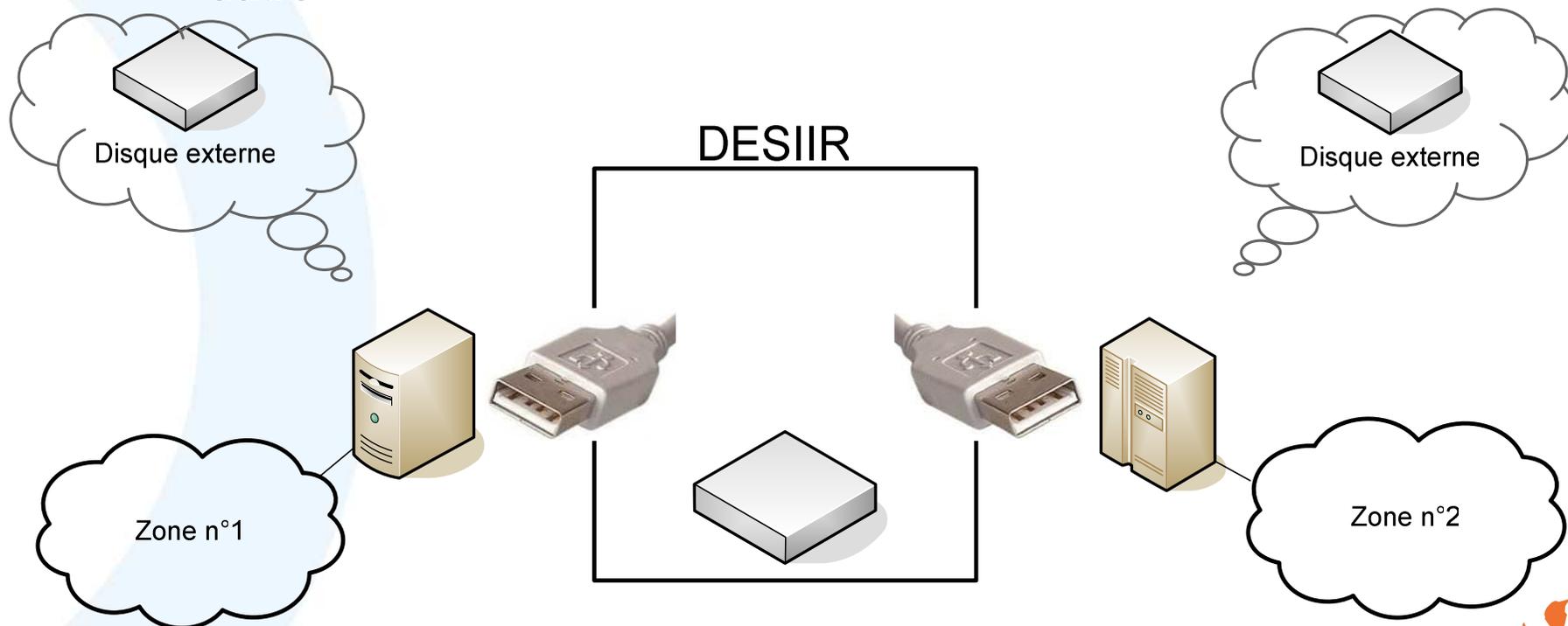
- ✿ **Besoin de confort** (par opposition au transfert hors-ligne, par ex. clé USB), Cf. « le réseau avec les pieds » des supports physiques !
 - Doit fonctionner sur ≠ systèmes, « plug & play »
 - Ne doit pas nécessiter de compétences particulières en sécurité / réseau pour l'installation et l'utilisation



Vue fonctionnelle : « sas disque dur »

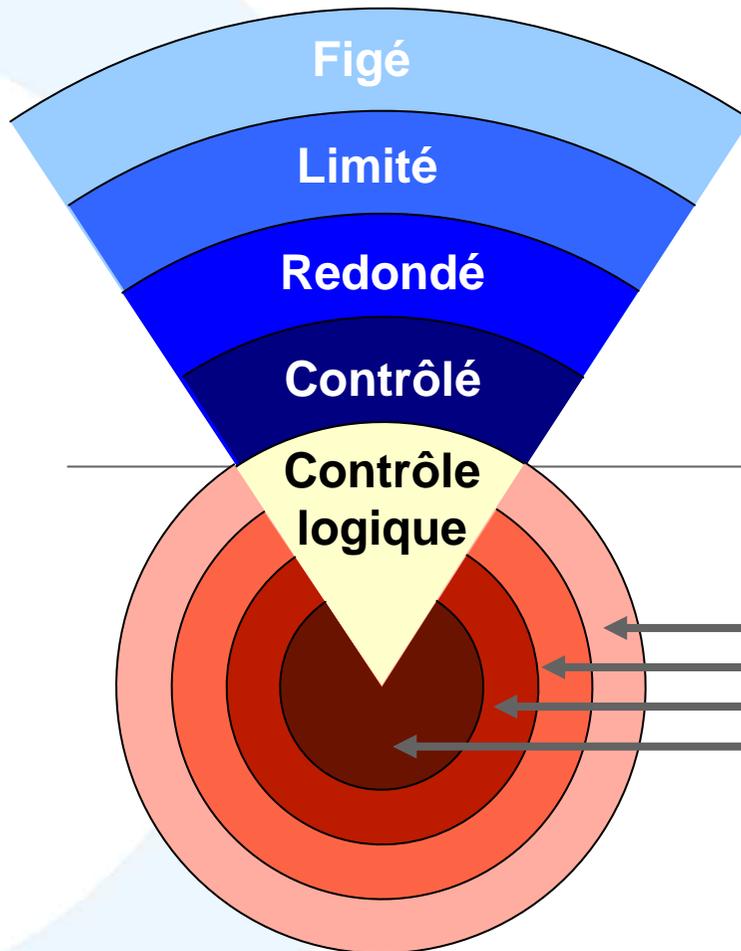
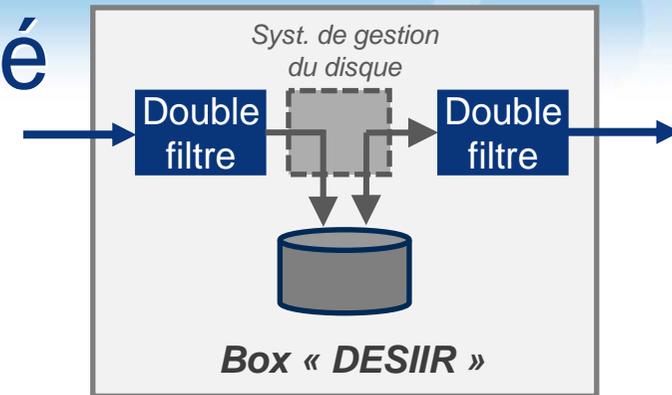
Cible de sécurité

- Transférer de l'information entre deux zones en garantissant une « assurance raisonnable » de non-intrusion d'une zone vers une autre





Mécanismes de sécurité



❁ Défense en profondeur

- Composants reprogrammés et figés
- Protocoles bas niveau mono-fonctionnels limités
- Diversification (ex : opérations de filtrage redondées sur des équipements différents)
- Contrôle d'accès au niveau composant (R, W, RW)

❁ Contrôle de contenu

- Noms et extension des fichiers
- Taille fichier, longueur des lignes
- Caractères autorisés : uniquement ASCII imprimables
- Validation de la syntaxe (format autorisé)
- *Conserve la validation humaine (validation du sens)*



Couverture des besoins par différentes solutions

	Sécurité physique	Sécurité contenu	Fiabilité	Confort
Diode physique	Unidirectionnel	Sécurité logique	Pas de garantie	
Transfert clé USB	Aucune connexion	Virus		Manipulations
Classique (DMZ, relais applicatif)	Sécurité logique	Sécurité logique		
DESIIR	✓	✓	✓	✓



Contact : desiir@edf.fr

 Prototype en cours



 Démarche de certification sécurité

- **DCSSI : Certification Sécurité de Premier Niveau (CSPN)**
- **Cible de sécurité : Transférer de l'information entre deux zones en garantissant une « assurance raisonnable » de non-intrusion d'une zone vers une autre**

 Partage, retour d'expérience