



Liberté • Égalité • Fraternité

RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE LA DÉFENSE

Diode réseau & ExeFilter

SSTIC06 – 01/06/2006



DÉLÉGATION GÉNÉRALE POUR L'ARMEMENT

Philippe Lagadec
DGA / CELAR
philippe.lagadec (à) dga.defense.gouv.fr



2 projets: Diode réseau & ExeFilter

- 2 projets du CELAR pour bâtir des **interconnexions sécurisées** entre un réseau sensible et un réseau de confiance moindre (i.e. Internet)
- **Diode réseau:**
 - Pour garantir des transferts unidirectionnels de données.
- **ExeFilter:**
 - Pour filtrer des fichiers et courriels, afin de supprimer tout contenu exécutable, et n'autoriser que des formats maîtrisés.
- Ces 2 types de produits n'existent pas aujourd'hui sur le marché français sous une forme satisfaisante pour nos besoins spécifiques.



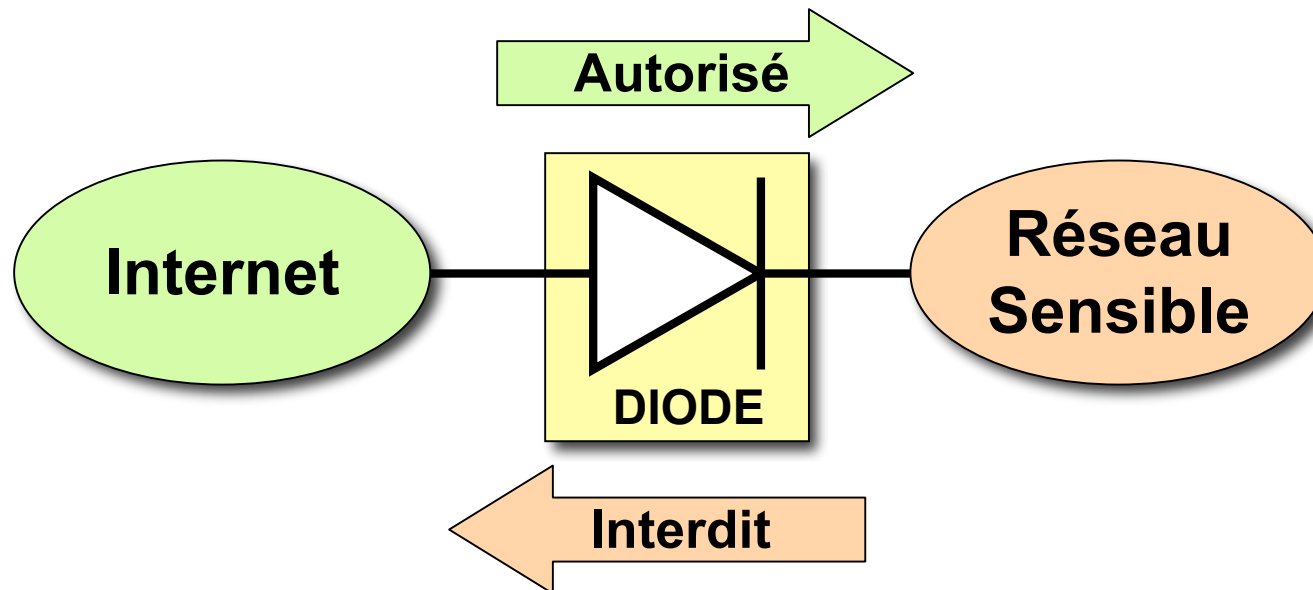
Diode réseau & ExeFilter

- Ces 2 projets sont indépendants et complémentaires:
 - La **Diode réseau** protège la **confidentialité** du réseau sensible par rapport à l'extérieur (sens montant).
 - **ExeFilter** contribue à protéger l'**intégrité** et la **disponibilité** du réseau sensible.
 - (...par rapport à l'interconnexion uniquement)



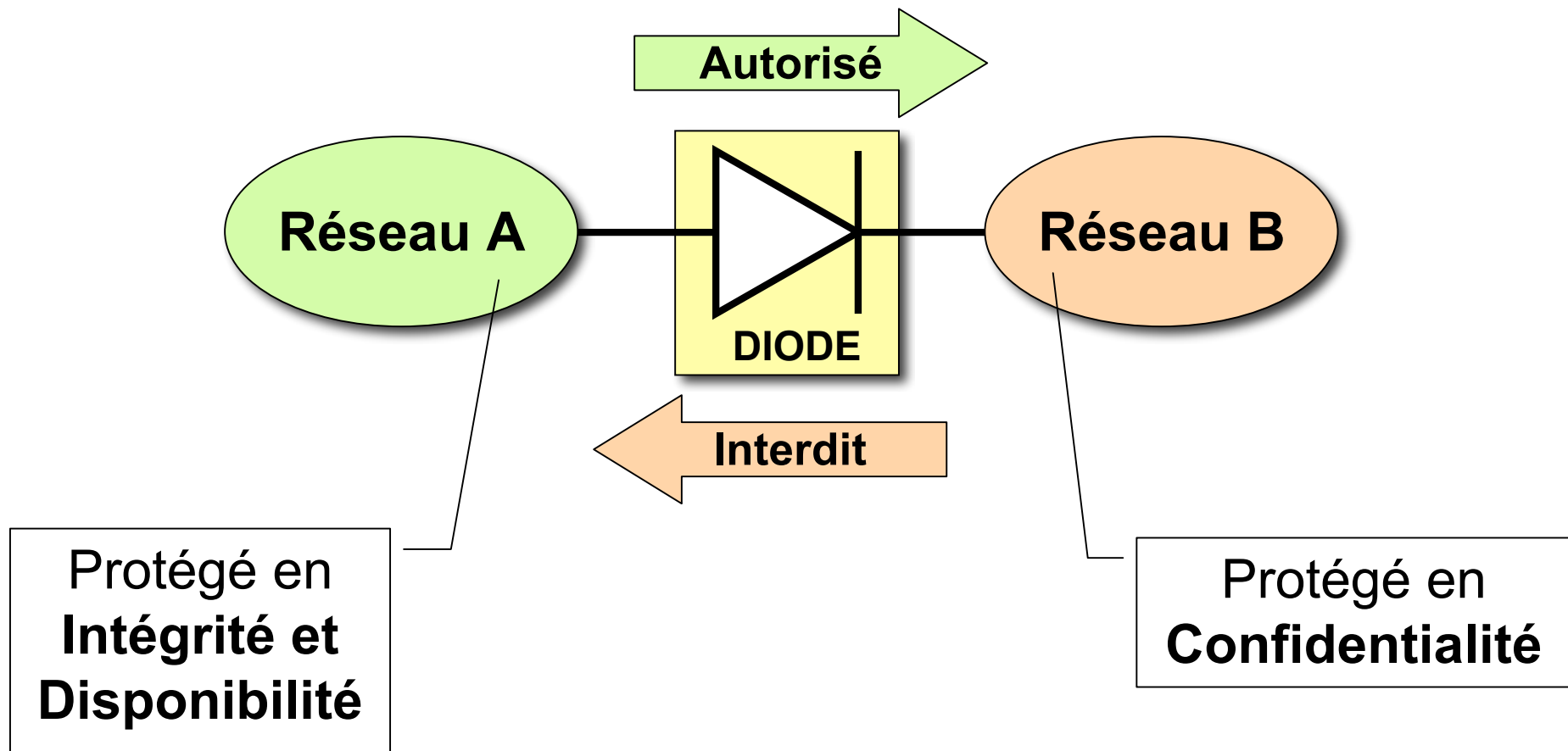
Diode réseau

- Pour interconnecter 2 réseaux de niveaux de sécurité différents.
- Pour échanger des informations **dans un seul sens, du bas vers le haut**.
 - Exemple: recopier des pages web ou des courriels vers un réseau sensible.





Diode – 2 utilisations possibles





Diode - Le besoin

- **Transfert de données pour divers services:**
 - Transfert de fichiers (automatisé ou non)
 - Synchronisation de répertoires
 - Transfert de courriels
 - Remontée d'événements: syslog, SNMP-Trap
 - Recopie de bases de données
 - ...

- Implémentation « **diode logique** » parfois possible avec un pare-feu classique (ou amélioré)
 - Cependant impossible de garantir à 100% sur le long terme l'absence de fuite d'information:
 - Vulnérabilités du logiciel pare-feu, des relais
 - Canaux cachés (signalisation, acquittements, commandes, ...)
 - Attaquant qui parvient à changer la configuration logicielle



Une diode réseau matérielle

- **Pour obtenir une confiance bien plus grande, des solutions matérielles existent:**
 - Liaison série RS-232 partielle
 - Liaison Ethernet cuivre RJ45 partielle
 - Liaison optique avec une seule fibre
 - ... ?

- **La liaison optique paraît la plus adaptée:**
 - Garantie de « non-réversibilité » (émetteur/récepteur)
 - Peu d'erreurs de transmission
 - Haut débit

- **Bien sûr une protection n'est jamais parfaite dans le monde de la sécurité**
 - Toujours possible de faire fuir de l'information via **la couche 8 du modèle OSI**, qui n'est pas (encore) filtrée par les IPS du marché.
 - (...l'utilisateur)



Diode - Notre solution technique

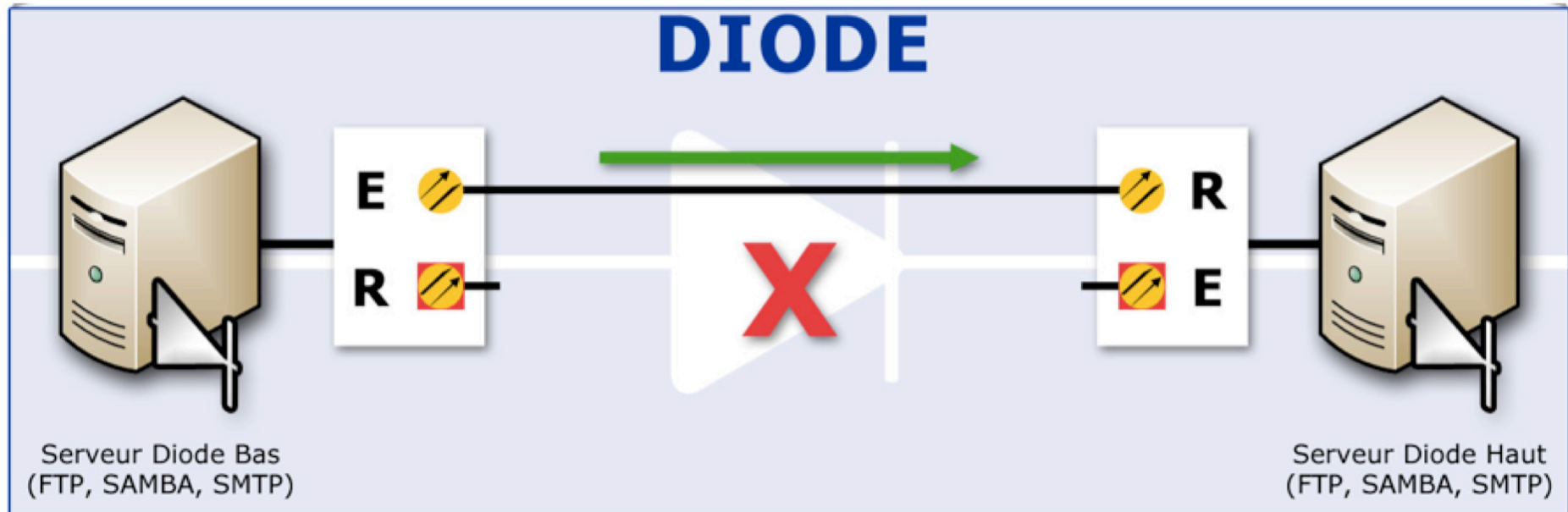
- **Le prototype de diode CELAR est basé sur 2 parties:**
 - **1) Une interconnexion physique** grâce à une simple fibre optique Ethernet entre 2 PCs.
 - (matériel standard peu onéreux)
 - **2) Un logiciel émetteur / récepteur** capable de transmettre des fichiers ou des courriels sans retour d'information.
- **Objectif:**
 - Montrer qu'une telle interconnexion est possible, **simple, sécurisée, et ne coûte pas plus cher que 2 PCs et quelques matériels réseau.**





Diode - historique

- **2002-2005: Diode CELAR v1, développée en C**
 - Débit satisfaisant: 8 Mbits/s pour des fichiers ou courriels
 - Manque de robustesse, code source et algorithmes complexes.
- **2005-...: Diode CELAR v2, réécrite en Python**
 - Algorithme beaucoup plus simple, portable Windows / Linux / MacOSX / ...
 - Débit utile obtenu: **12 Mbits/s**, sans optimisation particulière pour l'instant.
 - Développement à poursuivre: gestion des courriels, optimisations, robustesse, IHM, ...

▶ Diode – partie matérielle



E : Emetteur  : Fibre optique connectée
R : Récepteur  : Fibre optique non connectée

- 2 transceivers (convertisseurs) RJ45 cuivre / fibre optique, 1 seule fibre est connectée.



Diode – partie matérielle





Diode – démo partie matérielle

- Netcat serveur UDP sur PC diode haut:
 - `nc -l -u -p 1234 -v`
- Netcat client UDP sur PC diode bas:
 - `arp -s 192.168.1.101 01-23-45-67-89-AB`
 - (sous Windows)
 - `nc -u 192.168.1.101 1234 -v`
- => Une fois la fibre optique « sens descendant » débranchée, seul le PC diode haut peut recevoir des données.



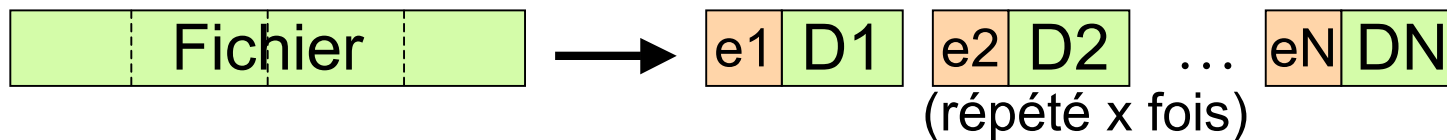
Contraintes techniques

- **Liaison parfaitement unidirectionnelle:**
 - Pas d'acquittement possible (pas de TCP)
 - => **UDP**
 - Pas de retransmission automatique en cas d'erreur ou de perte d'un datagramme
 - => **redondance nécessaire**
 - Entrée manuelle @MAC/@IP dans table ARP (ou bien broadcast Ethernet)
- Certains transceivers « intelligents » nécessitent un signal sur leur port RX pour émettre
 - Solutions: un 3^{ème} transceiver branché dans le vide, modification électronique, ...



Diode – partie logicielle (émetteur)

- **Emetteur sur serveur diode bas:**
 - Surveille un répertoire et détecte tout ajout ou modification de fichier.
 - Découpe chaque fichier à transmettre en datagrammes UDP
 - Entête: nom+chemin relatif du fichier, taille, date, position du datagramme, ...
 - **Transmet chaque datagramme 1 fois.**
 - **La redondance est assurée au niveau fichier, et non au niveau datagramme.**
 - Notre expérience montre que c'est beaucoup plus simple, et tout aussi efficace.
 - L'ensemble des fichiers peut être retransmis N fois, ou bien indéfiniment.





Diode – partie logicielle (récepteur)

Démo

- **Récepteur sur serveur diode haut:**
 - Reçoit les datagrammes
 - Les réassemble dans des fichiers temporaires
 - Quand un fichier est reçu en entier, il est recopié au bon endroit dans le répertoire de réception.
- Algorithme très simple, et pourtant efficace. 😊
- Protocole baptisé « **BlindFTP** »

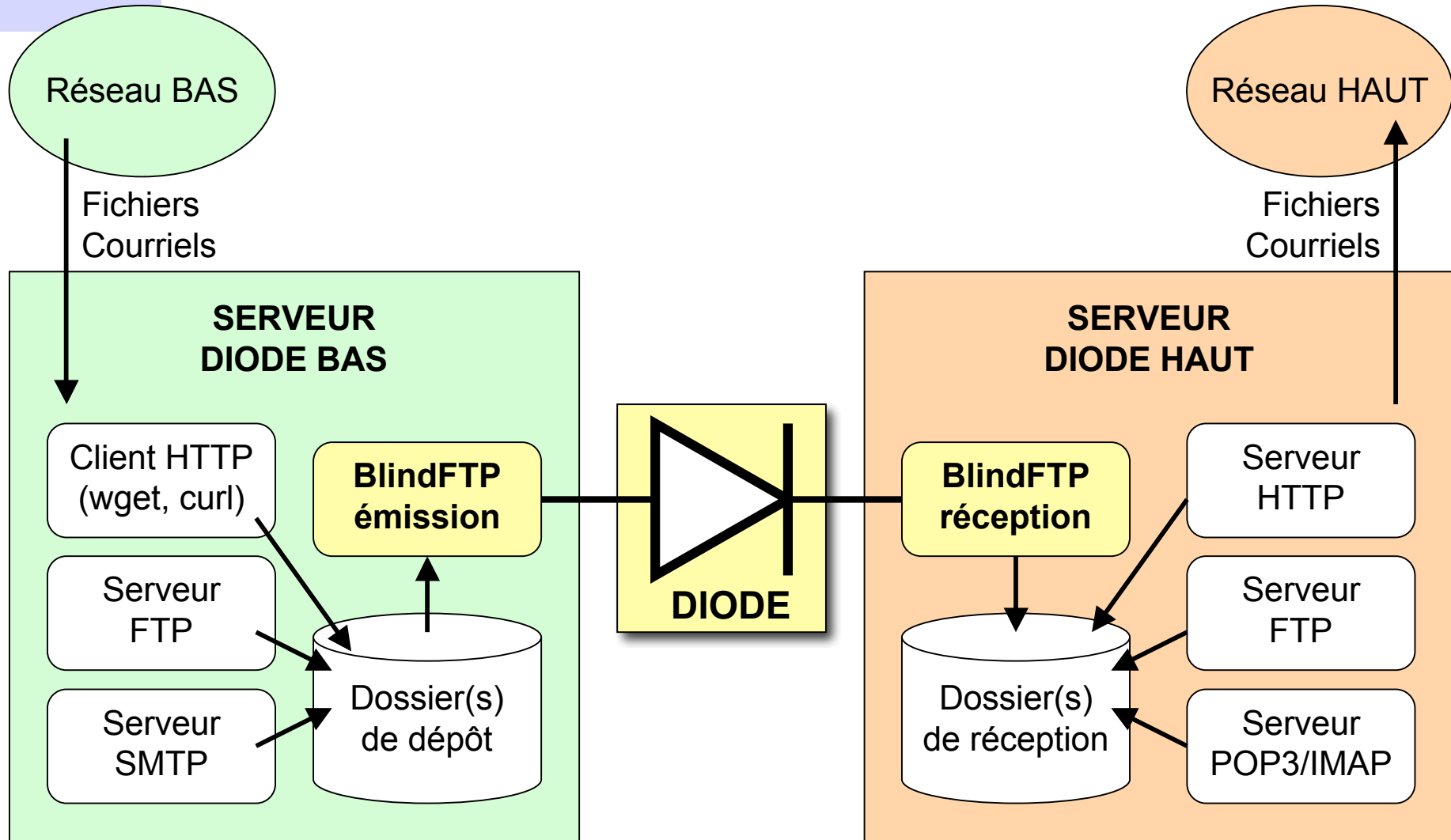


Optimisation des performances

- **Constat: certains datagrammes sont de temps en temps perdus**
 - le serveur haut est régulièrement occupé à autre chose (accès disque, IHM, lancement d'un autre logiciel, ...)
 - Les tampons de la pile IP se remplissent rapidement, les datagrammes suivants sont ignorés.
- **Solutions déjà employées:**
 - Augmenter la priorité du processus BlindFTP
 - Limiter le débit d'émission
- **Solutions envisagées:**
 - Augmenter la taille des tampons
 - Séparer la partie réception en plusieurs threads ou processus: réception UDP / décodage / écriture disque
 - Ajouter mécanisme de type FEC pour optimiser la redondance
 - FLUTE (RFC 3926) ou FCAST: transfert de fichiers unidirectionnel en multicast, avec FEC (Forward Error Correction) pour éviter redondance simple



Diode – Architecture de passerelle





Diode – Applications

- **Transfert simple de fichiers / répertoires:**
 - L'utilisateur dépose un fichier dans son répertoire « dépôt » côté bas. (via FTP, partage Windows, ...)
 - Il le récupère sur le réseau sensible quelques secondes plus tard dans son répertoire « import ».
 - Avantages:
 - Plus souple et plus sûr qu'un support amovible
 - Garantie de l'unidirectionnalité
 - Possibilité d'appliquer une politique de filtrage
 - Possibilité de tracer les imports de fichiers



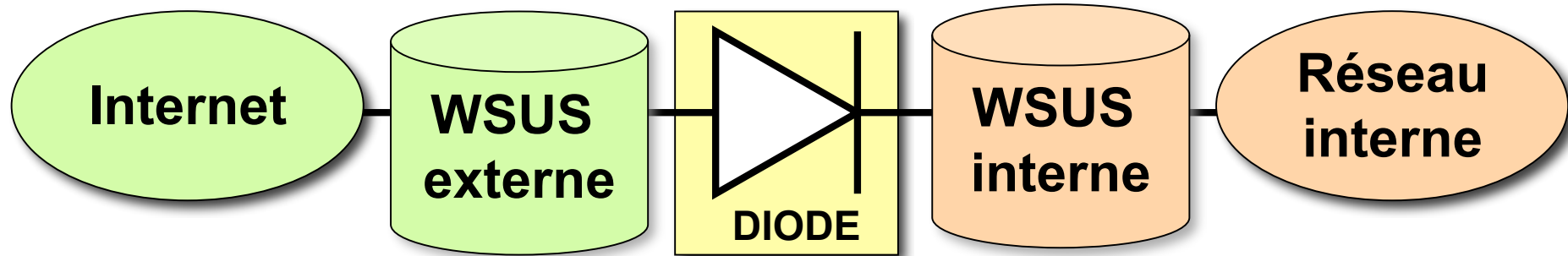
Diode – Applications

- **Recopie automatique de fichiers depuis Internet:**
- Application très utile pour **automatiser les mises à jour:**
 - de **signatures antivirus**
 - de **Windows (Double serveur WSUS)**
 - de **Linux, BSD, ...**
 - d'**outils de sécurité**: Nessus, HFNetChk, Snort, ...
- ... le tout sans une connexion Internet complète
- Killer-app pour un réseau sensible !



Exemple : Mises à jour Microsoft

- **WSUS: Windows Server Update Services**
 - un serveur connecté à Internet télécharge automatiquement toutes les mises à jour Microsoft choisies (sélection des OS et produits, des langues, ...)
- **Export régulier de la base de données des correctifs:**
 - `WSUSutil.exe export wsus.cab wsus_export.log`
- **Transfert par la diode (base exportée + correctifs)**
 - Environ 20 Go pour tous produits Microsoft (fr+us)
- **Import BD sur un 2ème serveur WSUS interne:**
 - `WSUSutil.exe import wsus.cab wsus_import.log`
- **Mise à jour des machines internes par Automatic Update** (activé par Stratégies de sécurité).





Diode - Autres applications possibles

- Recopie de sites web (wget)
- Transfert de messagerie
- Synchronisation de base de données
- Remontée d'alertes
 - Par messagerie, syslog ou SNMP-Trap
- Sauvegarde d'événements dans un « sanctuaire »
- IDS furtif
- Honeypot furtif ?
- ...
 - (tout autre protocole qui peut être converti en flux unidirectionnel)



Diode réseau – bilan

- **Partie matérielle = sécurité**
 - (confidentialité uniquement)
- **Partie logicielle = services**
- Solution matérielle efficace et peu coûteuse pour une liaison diode:
 - 2 PCs, 2 ou 3 convertisseurs (100 à 200€ pièce)
- Logiciel de transfert très simple

- Cette diode réseau permet d'imaginer de nouvelles applications pour des réseaux sensibles ne pouvant être connectés « normalement » à Internet:
 - Mises à jour automatiques, transferts de données, ...

ExeFilter

Un filtre générique d'analyse de contenu
pour les fichiers et courriels



Menace applicative

- **De nombreux formats de fichiers et de pièces jointes peuvent contenir du code malveillant camouflé (cheval de Troie):**
 - **Macros** ou **objets OLE** dans les documents Word, Excel, ...
 - **Scripts** dans les pages HTML, PDF
 - **Exécutables**
 - => cf. SSTIC03 et SSTIC04
- **Attaque applicative:** C'est souvent le dernier moyen qu'il reste à un attaquant pour pénétrer un système lorsque tout est bien sécurisé.

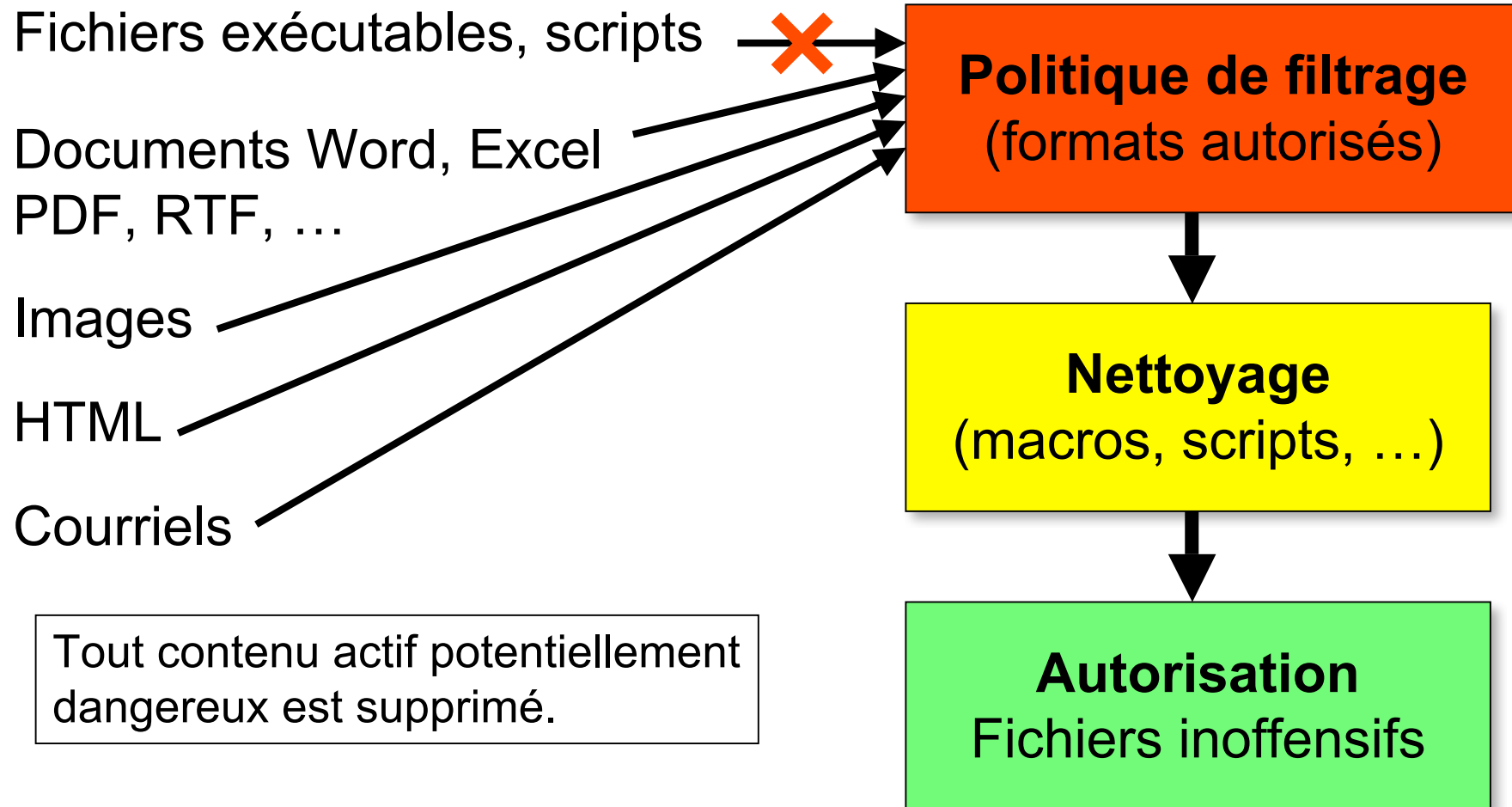


ExeFilter – l'objectif

- ExeFilter a pour but d'analyser et de filtrer ces fichiers, pour n'autoriser que des **formats maîtrisés et inoffensifs**.
- Objectif: appliquer une **politique de filtrage stricte, qui consiste à supprimer tout code exécutable ou contenu actif**.
 - => protection contre l'intrusion de chevaux de Troie ou de vers, virus, ...
 - Contraignant: pas applicable à tous les systèmes.
- Complémentaire de la diode, ou d'une passerelle bidirectionnelle.



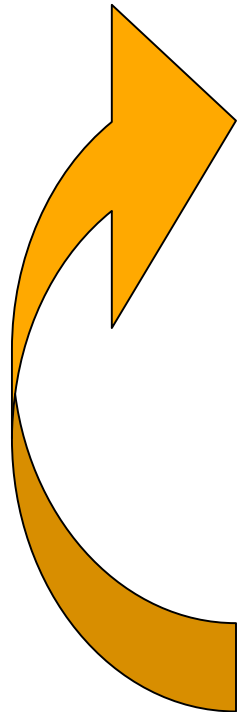
ExeFilter – politique de filtrage





ExeFilter – principe

Démo



- **Chaque fichier est analysé:**
 - **Détection du format** suivant son **nom** et son **contenu**.
 - **Refusé** si format interdit par la politique.
 - Exécutables, scripts, formats inconnus, chiffrés, ...
 - **Nettoyé** s'il contient du code actif
 - Macros dans docs Office, scripts dans HTML, ...
 - **Accepté** tel quel si inoffensif
 - Texte simple, images bitmap, ...
 - **Analyse récursive** si conteneur (archives Zip, ...)
- Concrètement, chaque filtre associé à un format donné est appelé en fonction du nom du fichier.
 - Exemple: rapport.doc → filtres Word, Texte et RTF



Détection de format

- Méthode choisie: **Liste blanche**
 - Tout ce qui n'est pas autorisé est interdit.
- 1. **Analyse du nom de fichier:**
 - => sélection de formats correspondants
 - Exemple: si « *.doc »: format Texte, RTF ou Word.
- 2. **Analyse du contenu:**
 - Chaque filtre sélectionné vérifie les données.
 - Exemple: un fichier Word doit commencer par « D0CF », un fichier texte ne doit pas contenir de caractères binaires.
 - Suivant la politique: acceptation, nettoyage ou blocage.



Formats de fichiers pris en charge

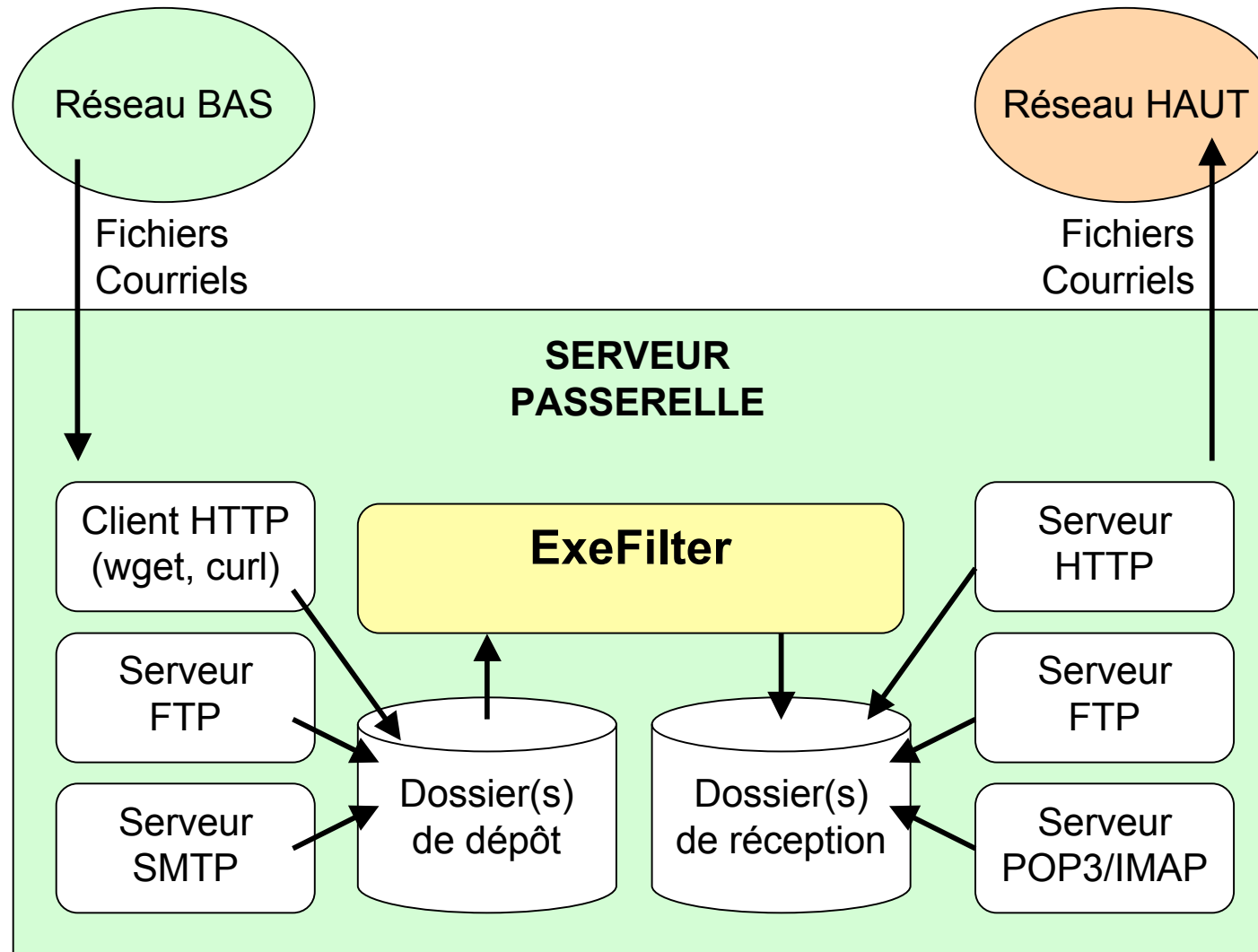
- Liste volontairement limitée à quelques formats répandus pour l'instant:
 - **BMP, JPEG, GIF, AVI, MP3, Texte**
 - **HTML, RTF, PDF**
 - **Word, Excel, Powerpoint**
 - **Zip, MIME**
- A ajouter:
 - XML, OpenDocument, Tar, Gzip, BZ2, ...



ExeFilter – Applications possibles

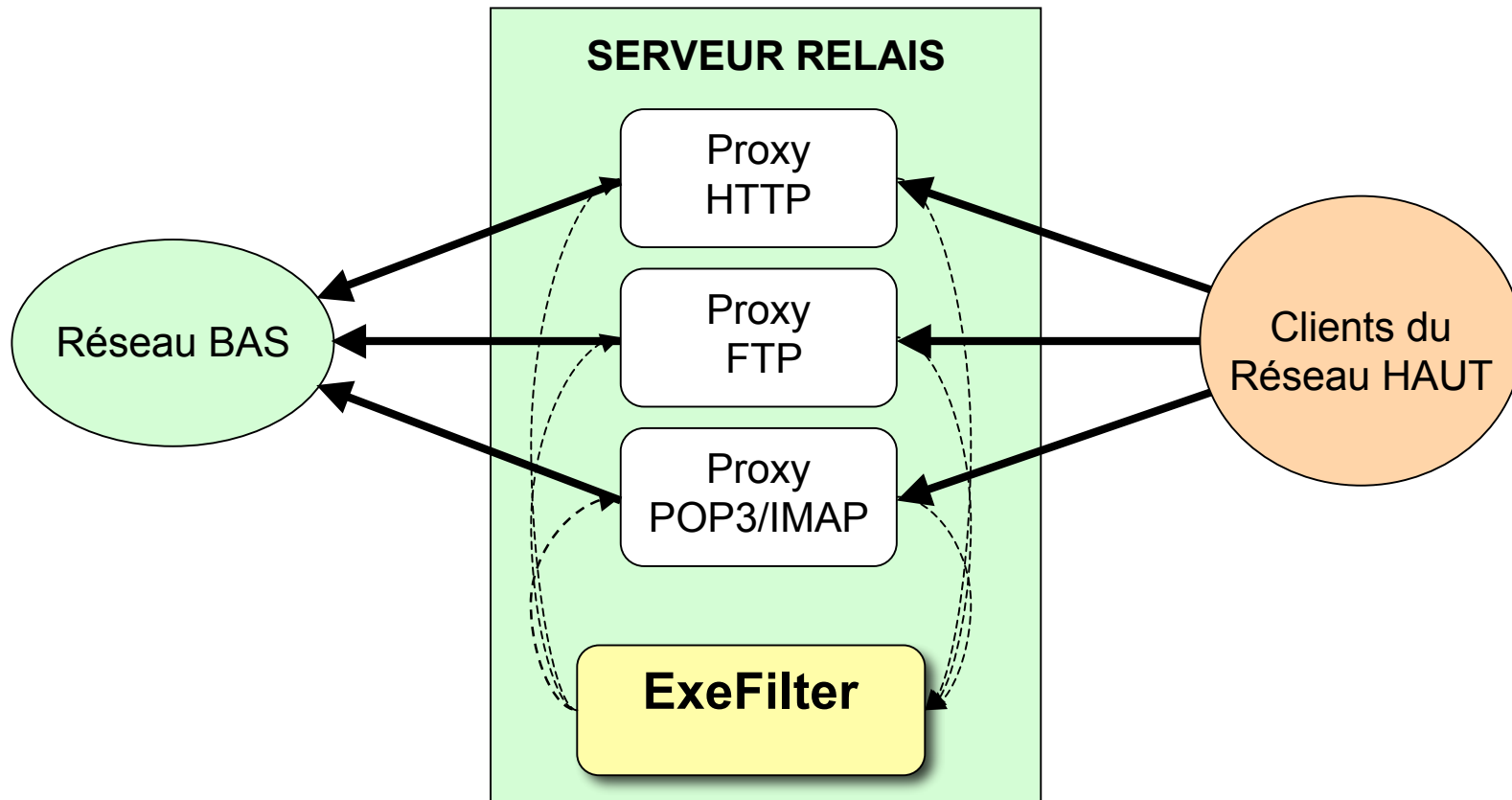
- **Passerelle de filtrage (proxy):**
 - Messagerie **SMTP**
 - Web **HTTP**
 - Transfert de fichiers **FTP**, Windows, ...
- **Sas de dépollution** pour supports amovibles
- **Protection locale** d'un poste client
 - (proxy POP3, IMAP, HTTP, FTP, ...)

ExeFilter – Passerelle entre serveurs



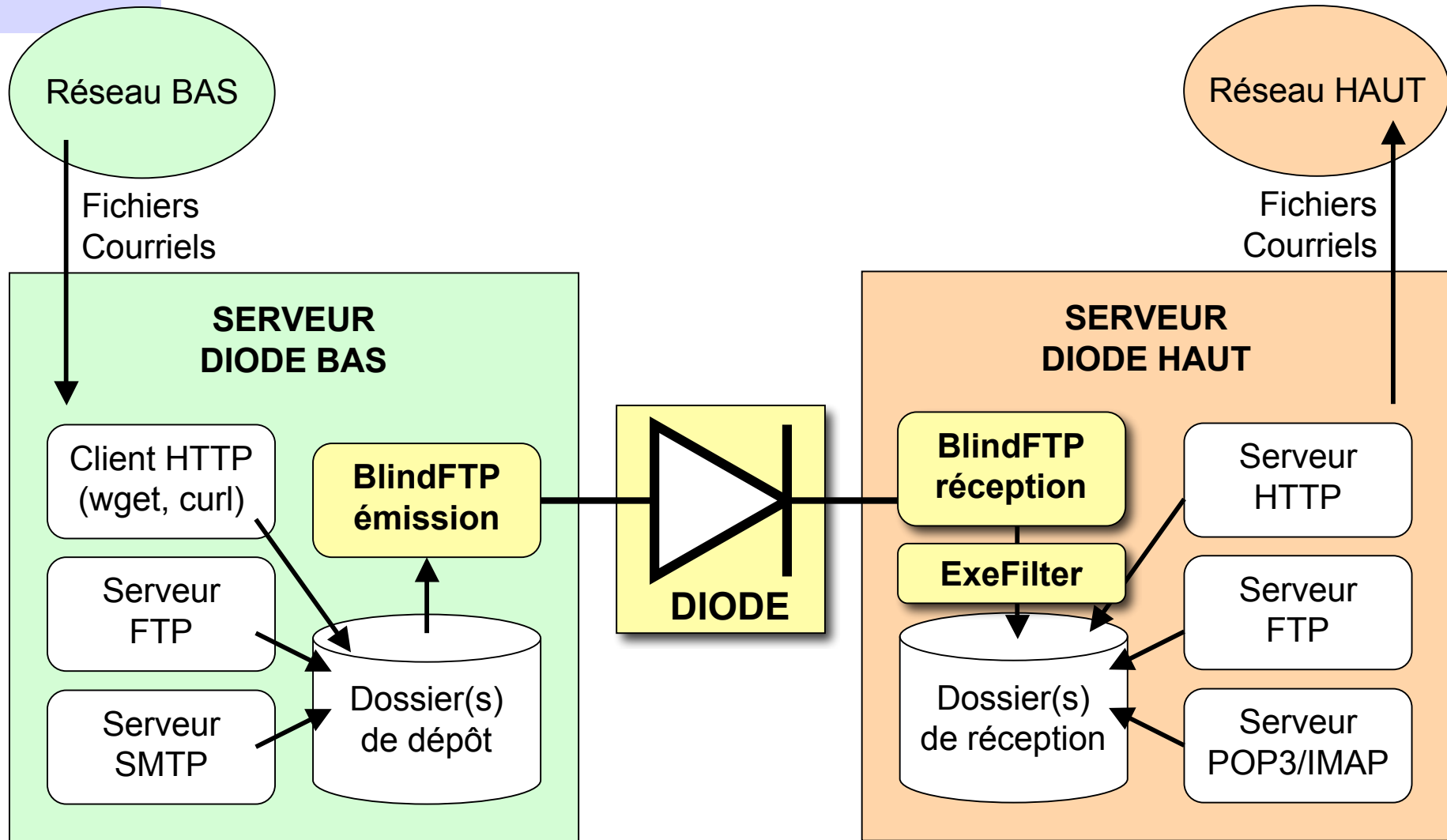


ExeFilter – Passerelle client/serveur





Passerelle Diode + ExeFilter





Avantages d'ExeFilter

- Conception générique et modulaire
- Intégrable dans de nombreux projets, pour de nombreux services:
 - Transfert de fichiers (manuel, FTP, ...)
 - Messagerie
 - Web
 - ...
- Algorithme plus fiable que les COTS proposant une fonction comparable. (approche liste blanche)
- Bonnes performances.
- Code source simple à comprendre et maintenir.
 - (en langage Python ;-)



CONCLUSION

- ExeFilter et la Diode réseau sont 2 projets complémentaires du CELAR pour bâtir des interconnexions sécurisées.
 - Issus de besoins militaires, mais pouvant être très utiles pour d'autres applications.
- Il est envisagé de diffuser au moins une partie de ces projets en logiciel libre.
 - Par exemple sur <http://admisource.gouv.fr>
 - Si vous êtes intéressés pour participer au développement, contactez-nous:
 - philippe.lagadec (à) dga.defense.gouv.fr