Sécurité des applications

ScanDo-InterDo

Yves LE ROUX
Gheorghe MOGA

www.kavado.com

OSSIR 13 MAI 2002

La société KaVaDo™

- **Créée au 1er trimestre 2000 par:**
  - Tal Gilat, PDG
  - Yuval Ben-Itzhak, Directeur Technique
- **Financée par:**
  - 3i Ventures, Bank of America
- **Implantations**
  - Siége social à New York
  - Centre de R & D en Israël
  - Bureaux de vente: New York, Atlanta, Washington DC, Silicon Valley, Londres, Tokyo, Madrid, Paris

Evolution des Applications Web

Contenu Statique

Fichier Hypertexte

Milieu 80

HTTP 1.0

Protocole de transfert de fichier texte à travers une connexion TCP/IP

Contenu Dynamique

Scripts coté serveur

Milieu 90

HTTP 1.1 & SSL

Amélioration de la sécurité et de la gestion des caches

Contenu Personnalisé

Scripts Client-Serveur

Fin 90

Cookies, JScript

Contenu spécifique pour l'utilisateur permettant des transactions

Applications Web

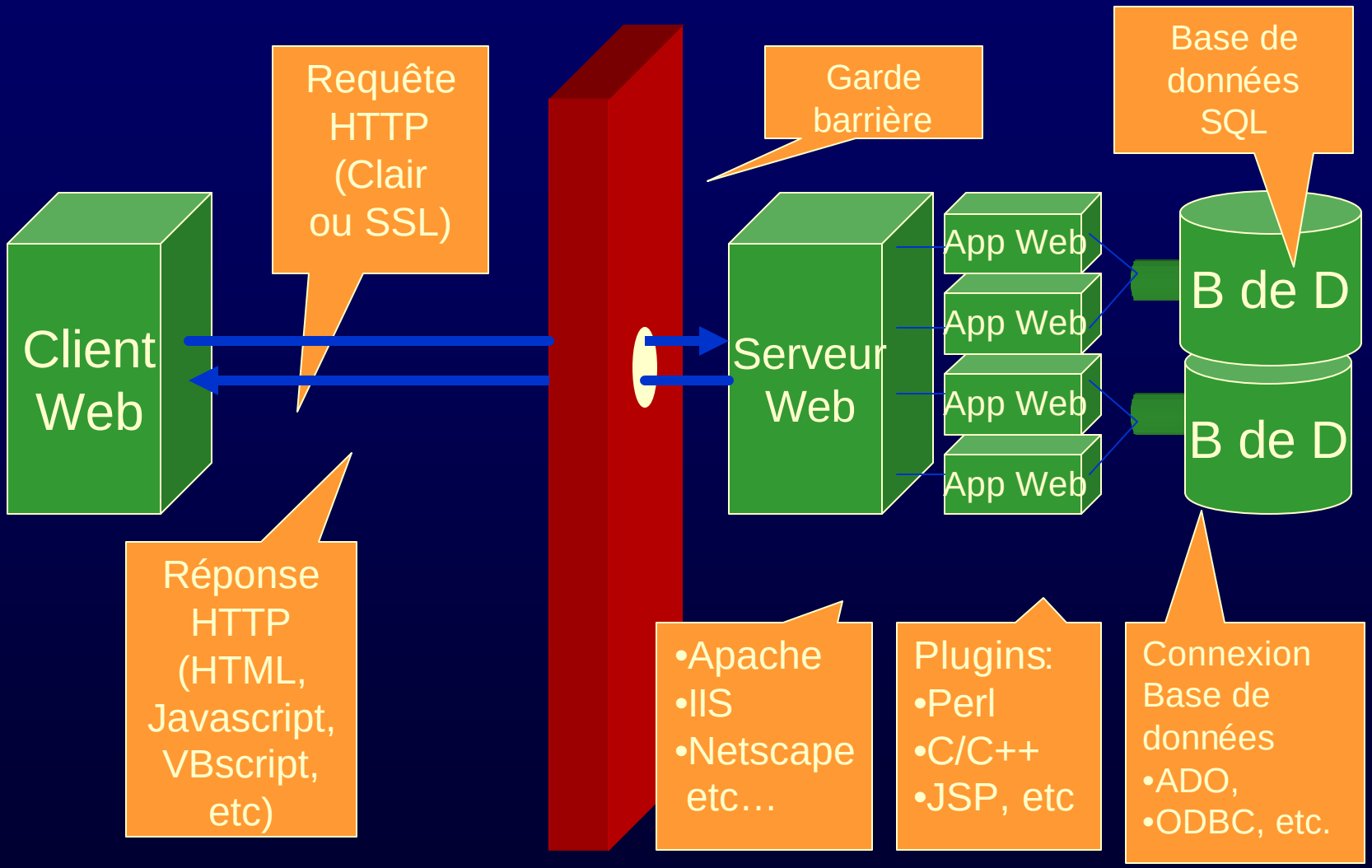
Extensions Client - Serveur

Debut 2000

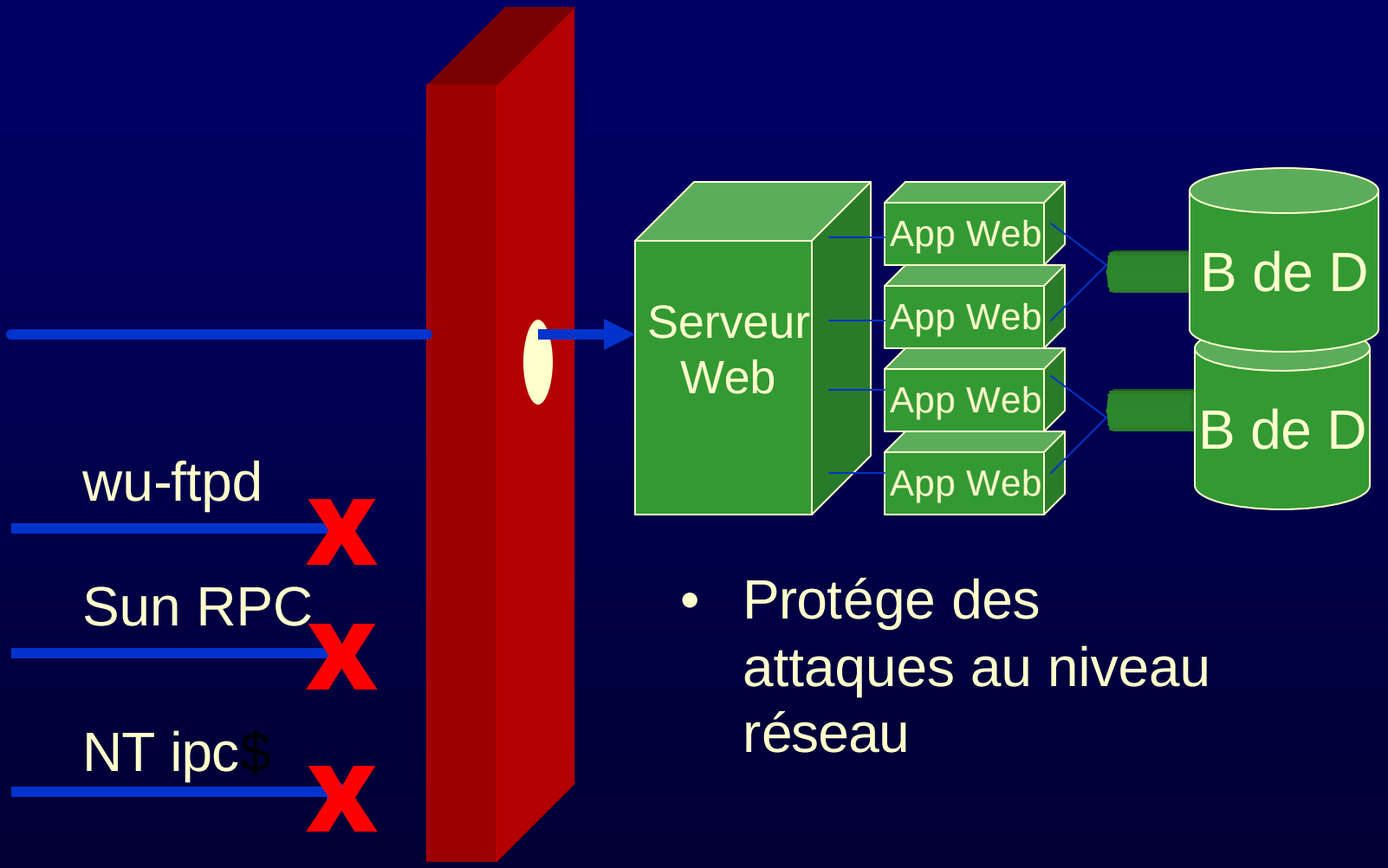
Base de données, Java, Flash

Transactions complexes avec paramétres et sessions multiples

Application Web Typique

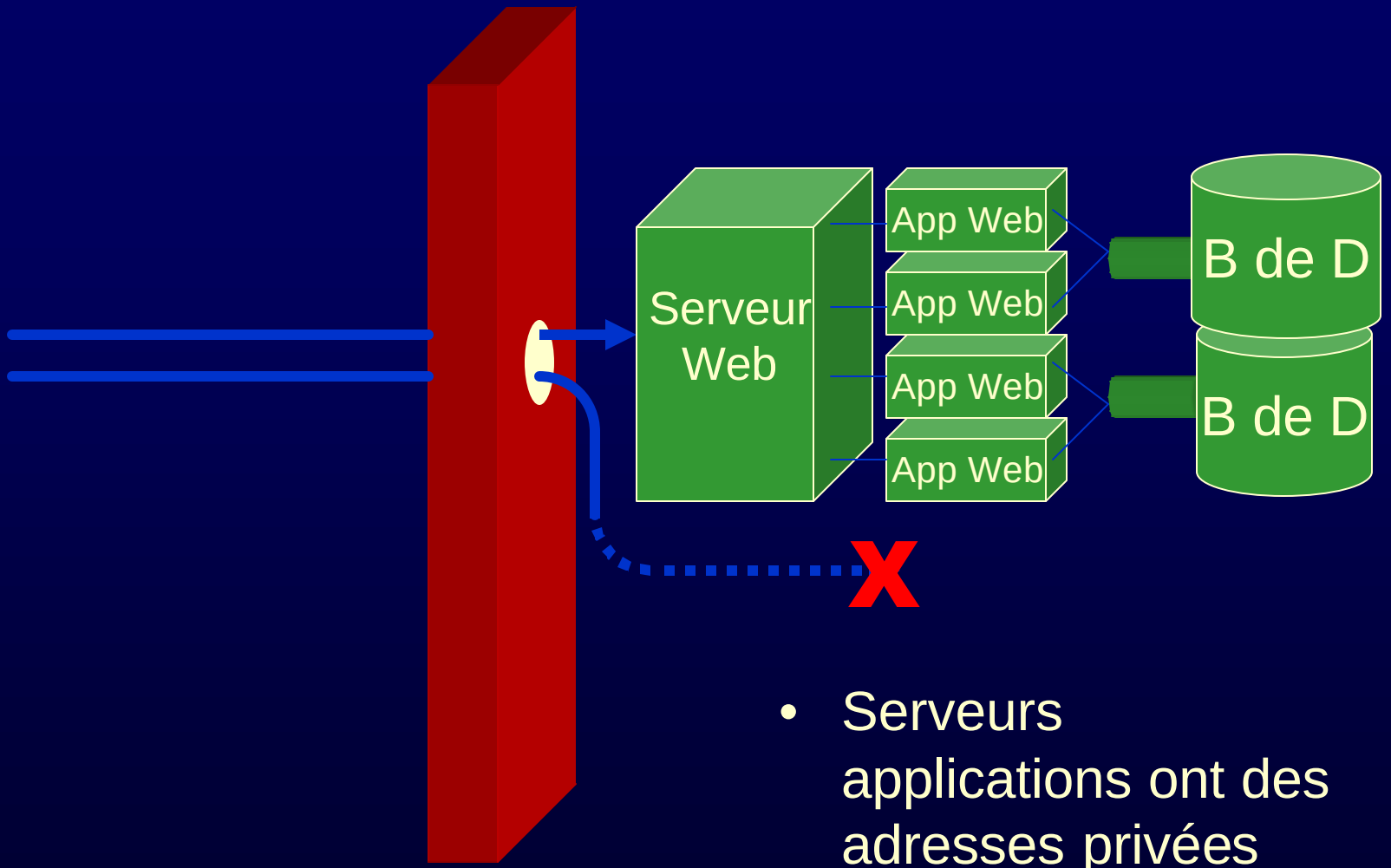


Utilité des gardes-barrières



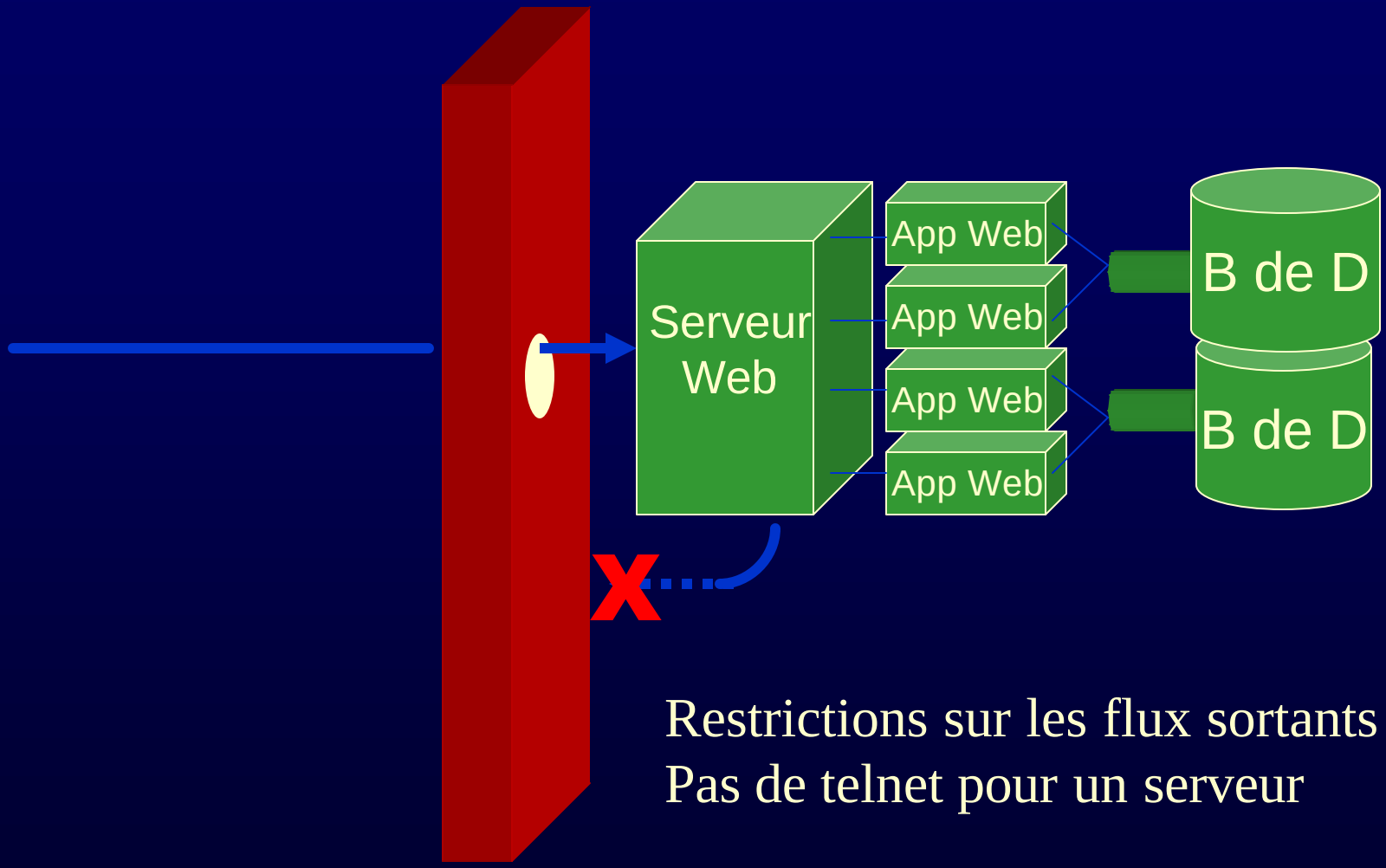
- Protége des attaques au niveau réseau

Utilité des gardes-barrières



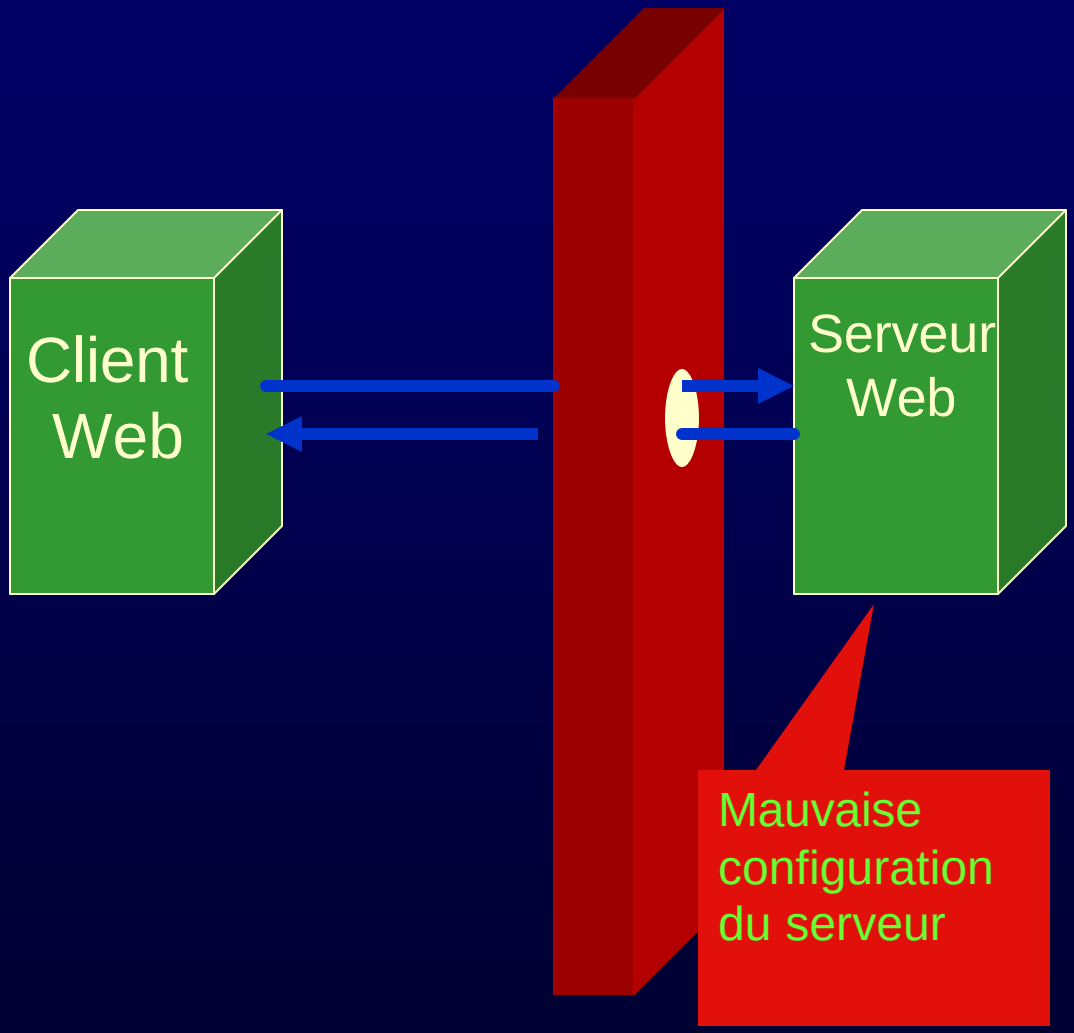
- Serveurs applications ont des adresses privées

Utilité des gardes-barrières

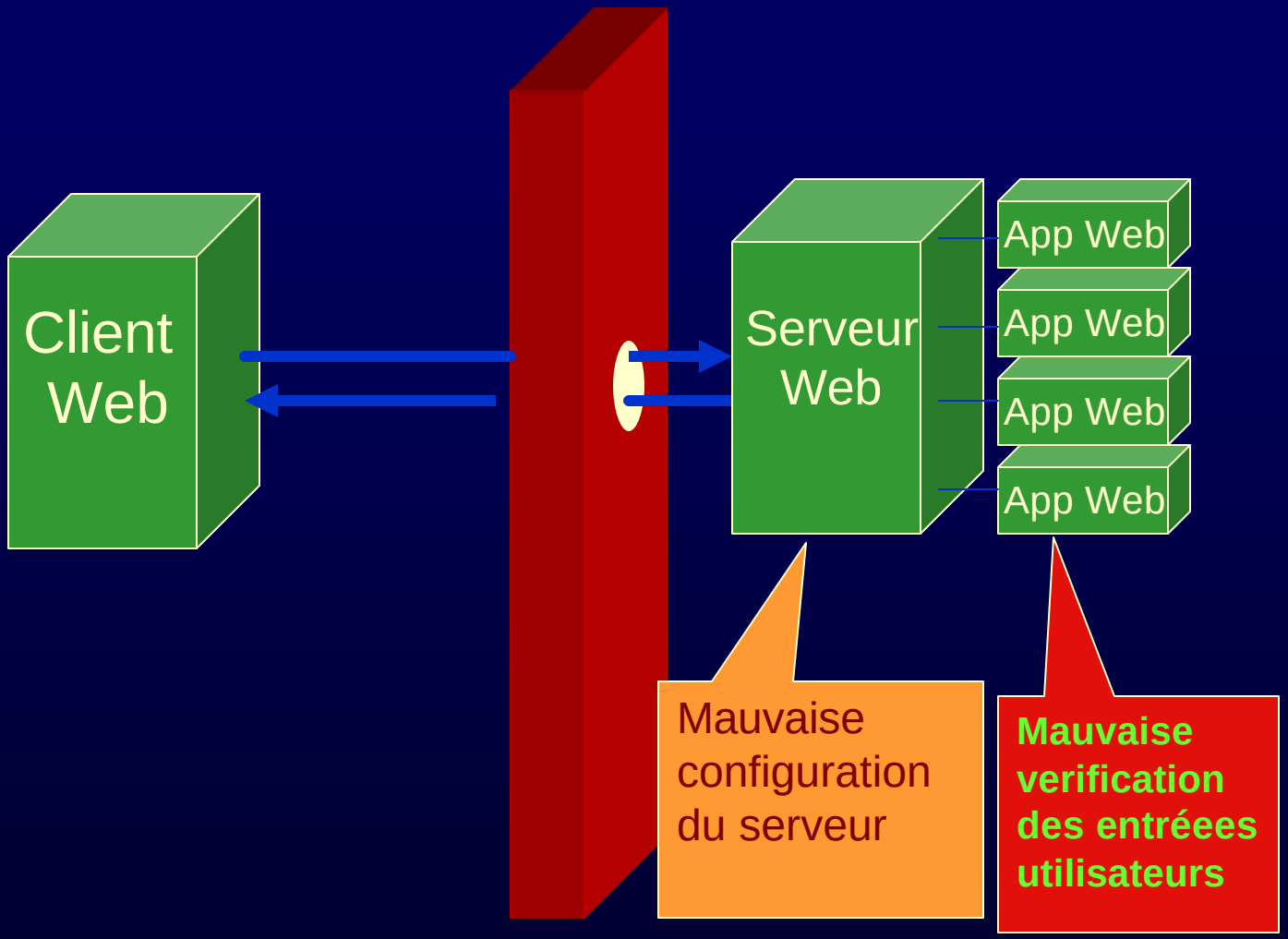


Restrictions sur les flux sortants
Pas de telnet pour un serveur

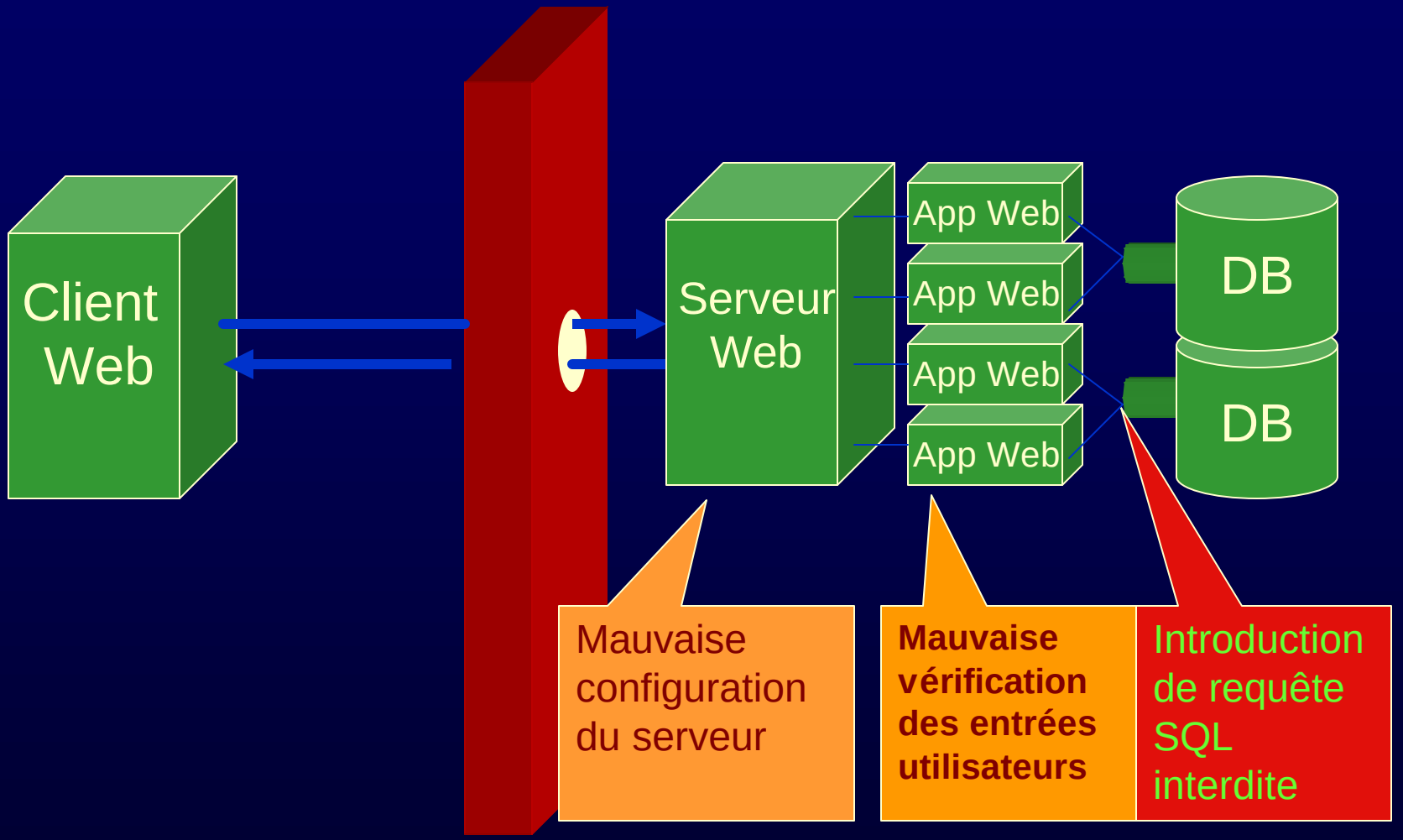
Ce que les garde-barrières ne peuvent pas éviter…



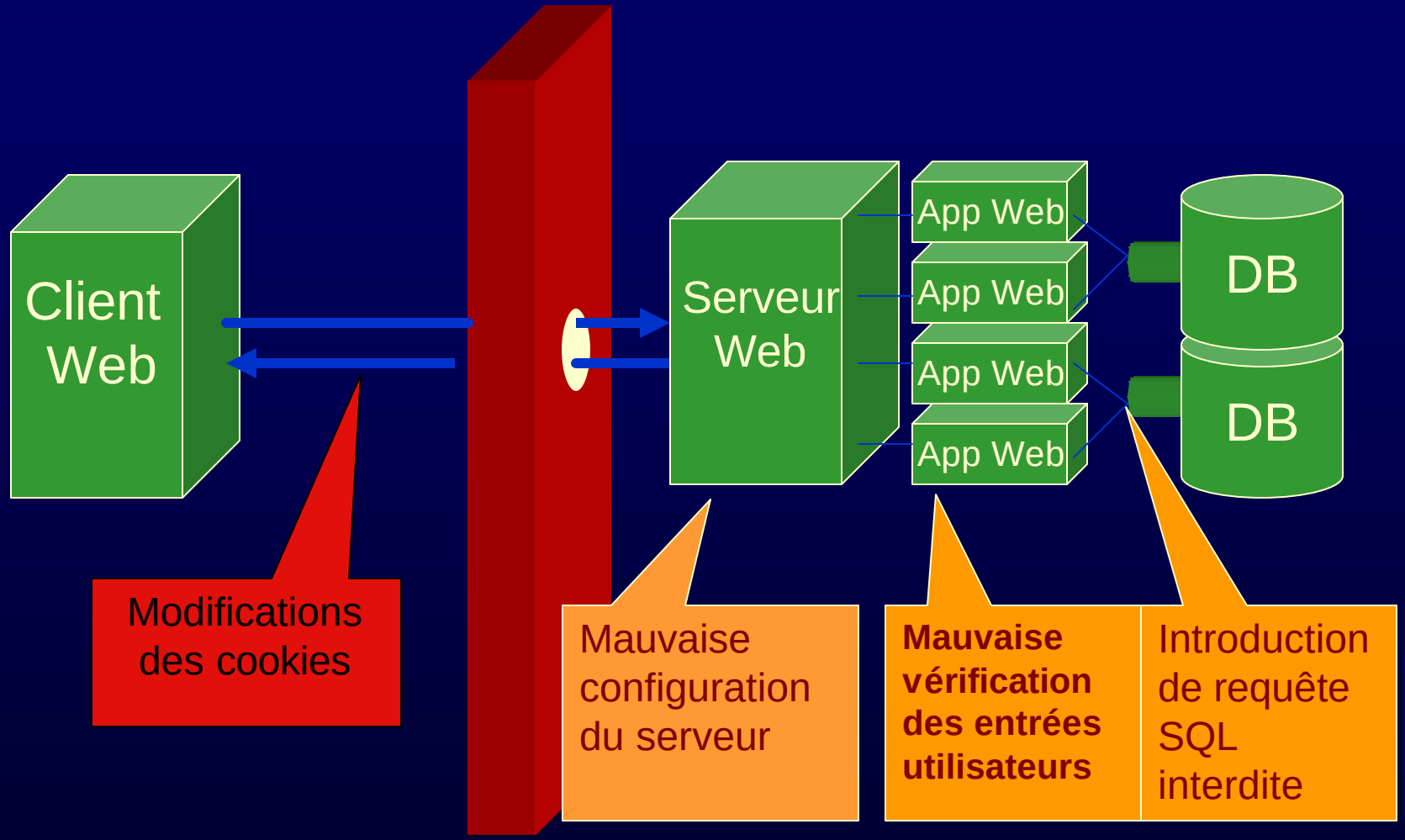
Ce que les garde-barrières ne peuvent pas éviter…



Ce que les garde-barrières ne peuvent pas éviter…



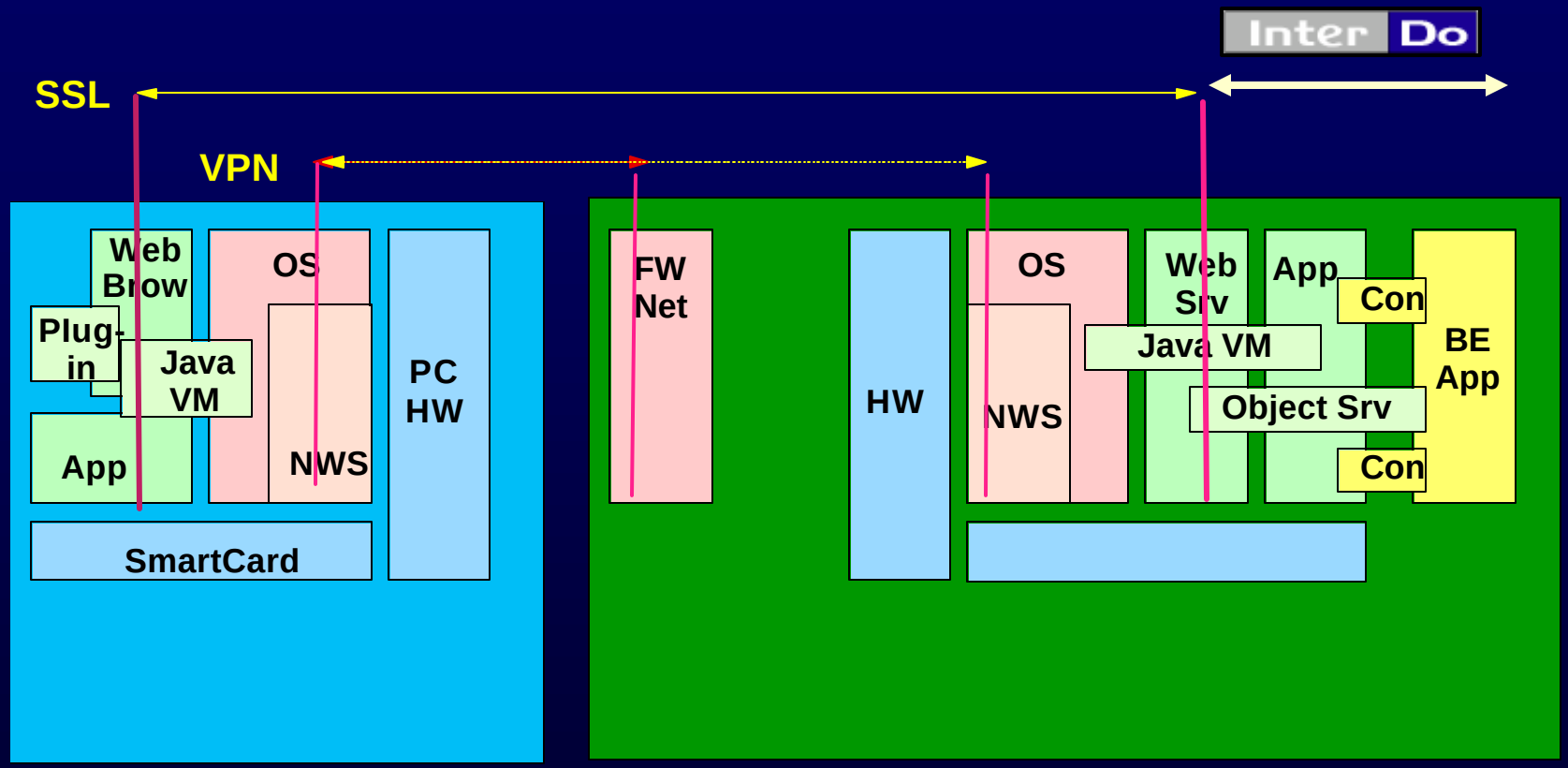
Ce que les garde-barrières ne peuvent pas éviter…



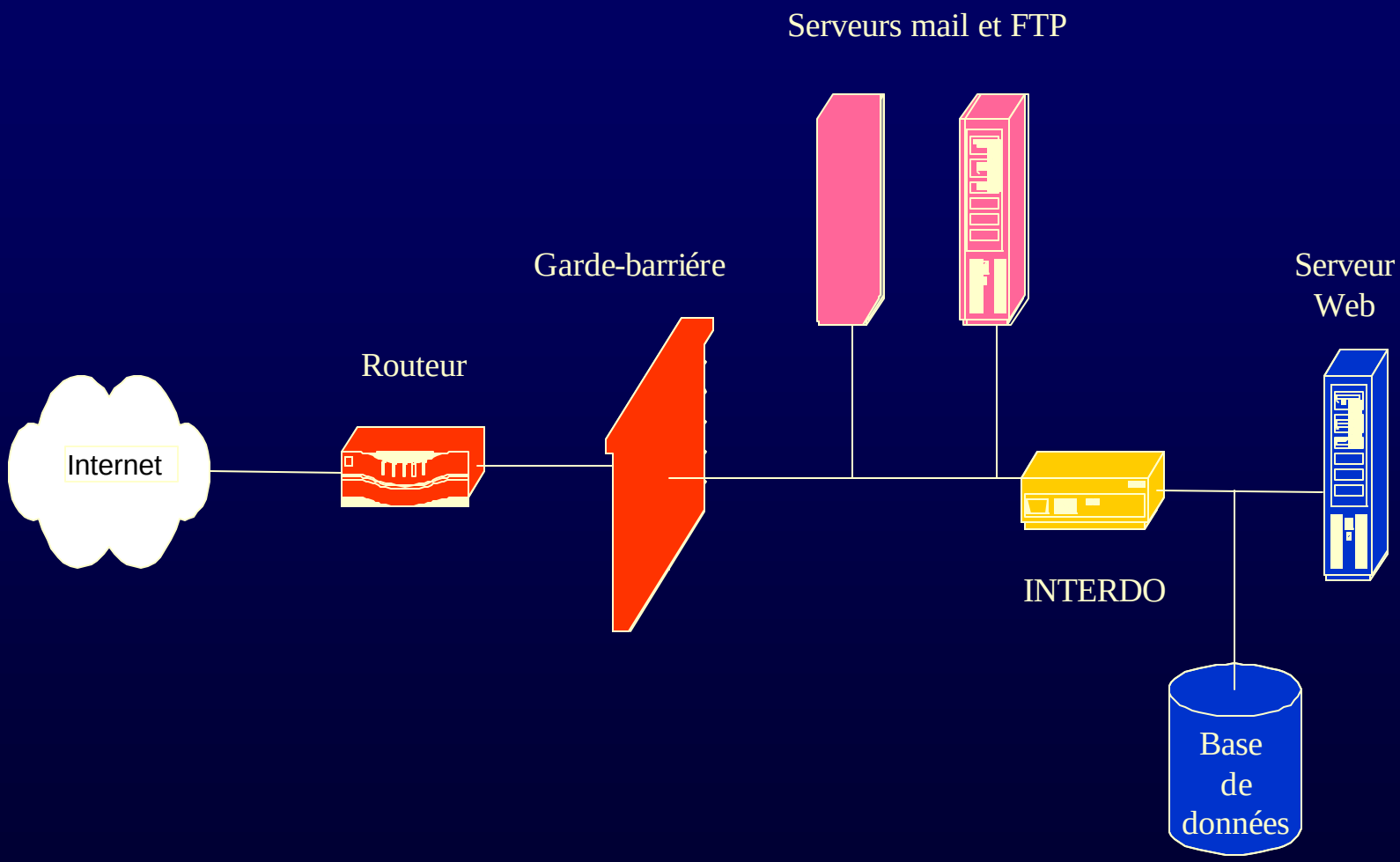
InterDo™

Protection des Applications Web

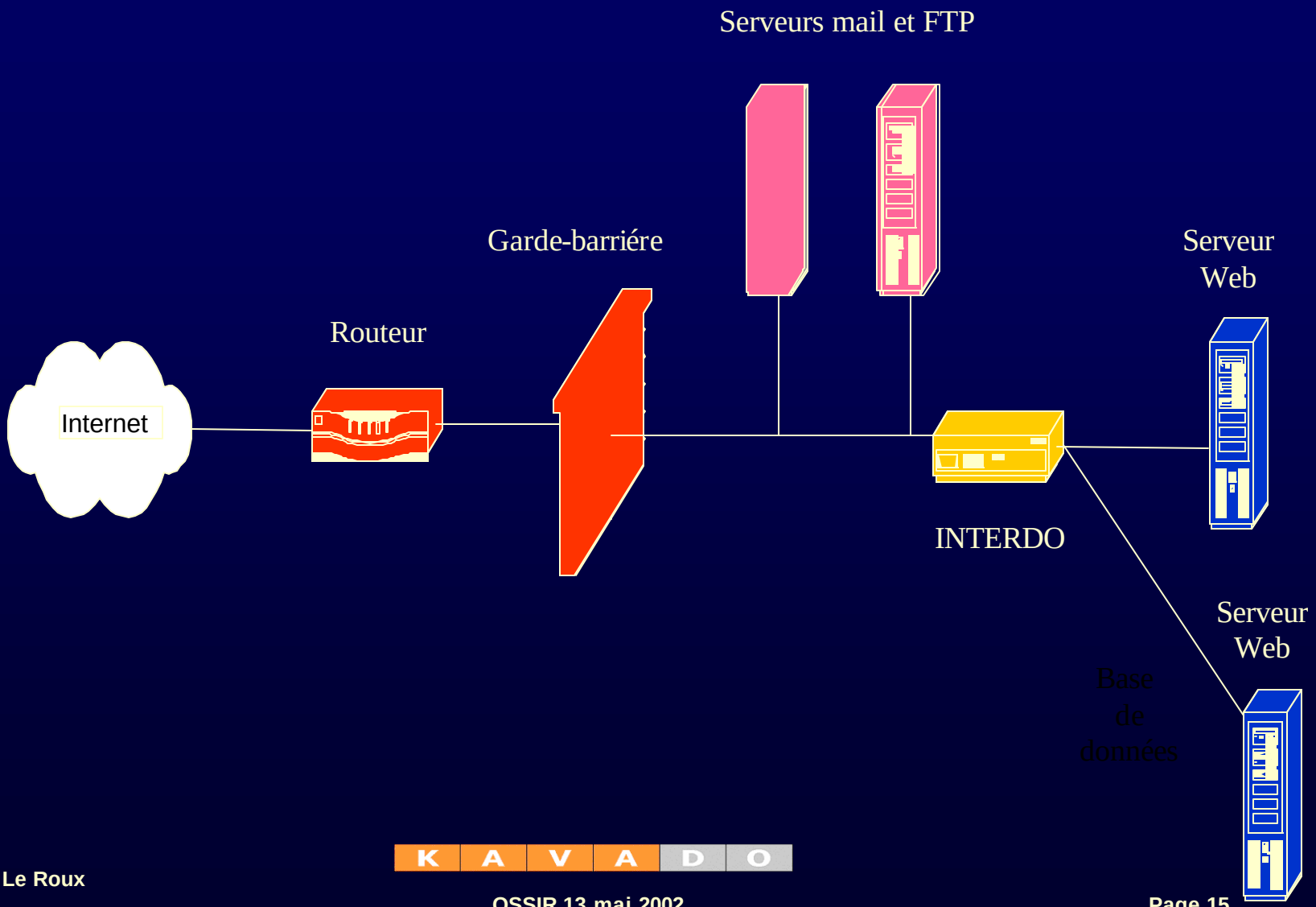
Sécurité classique: Garde-barrières + SSL



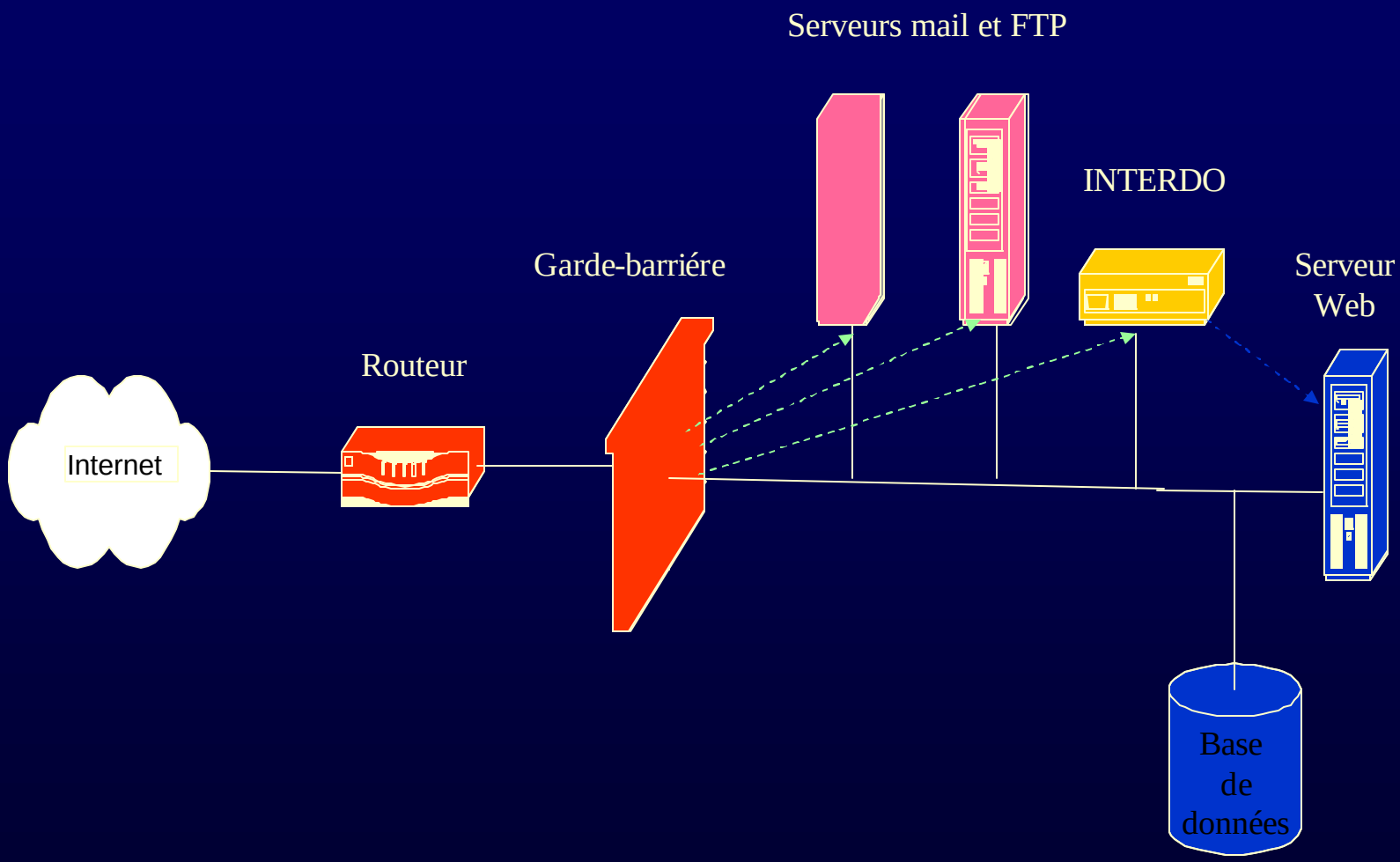
Topologies: Segment séparé



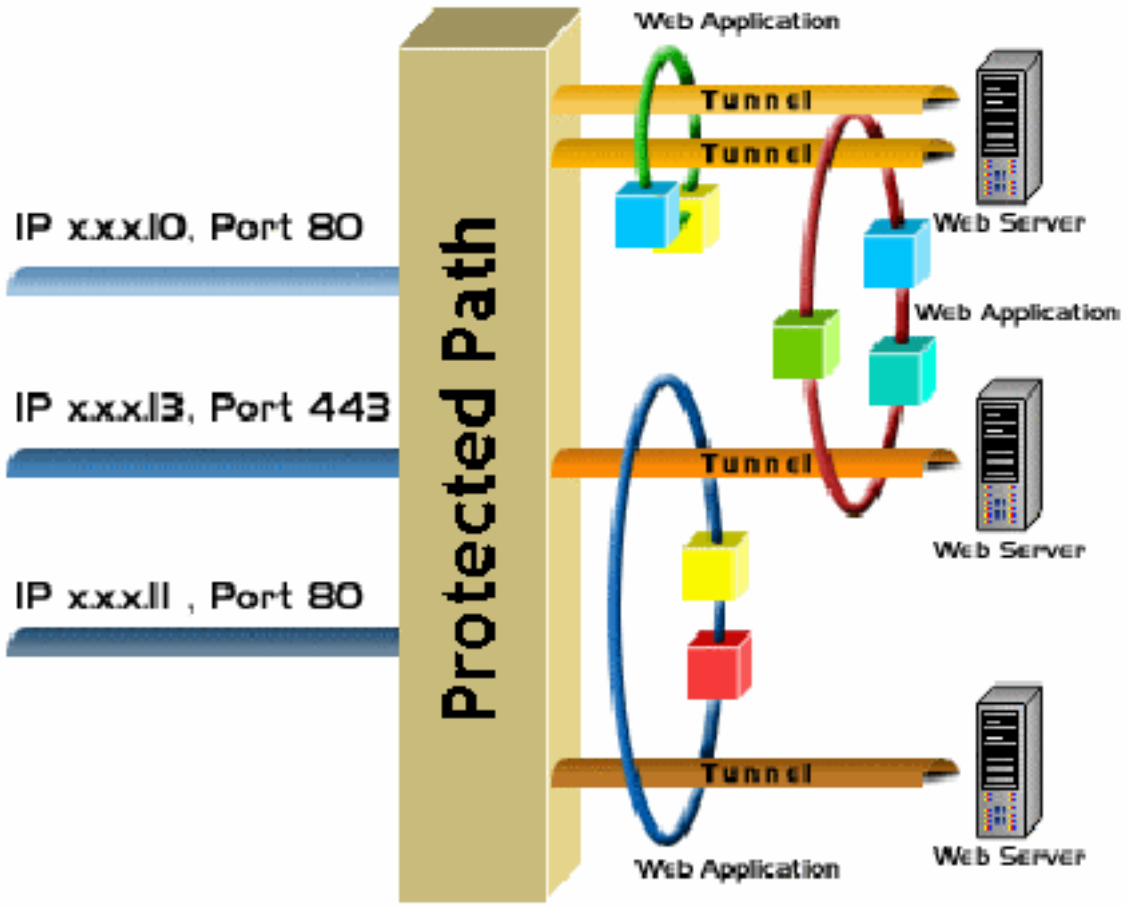
Topologies: 1 InterDo pour plusieurs serveurs



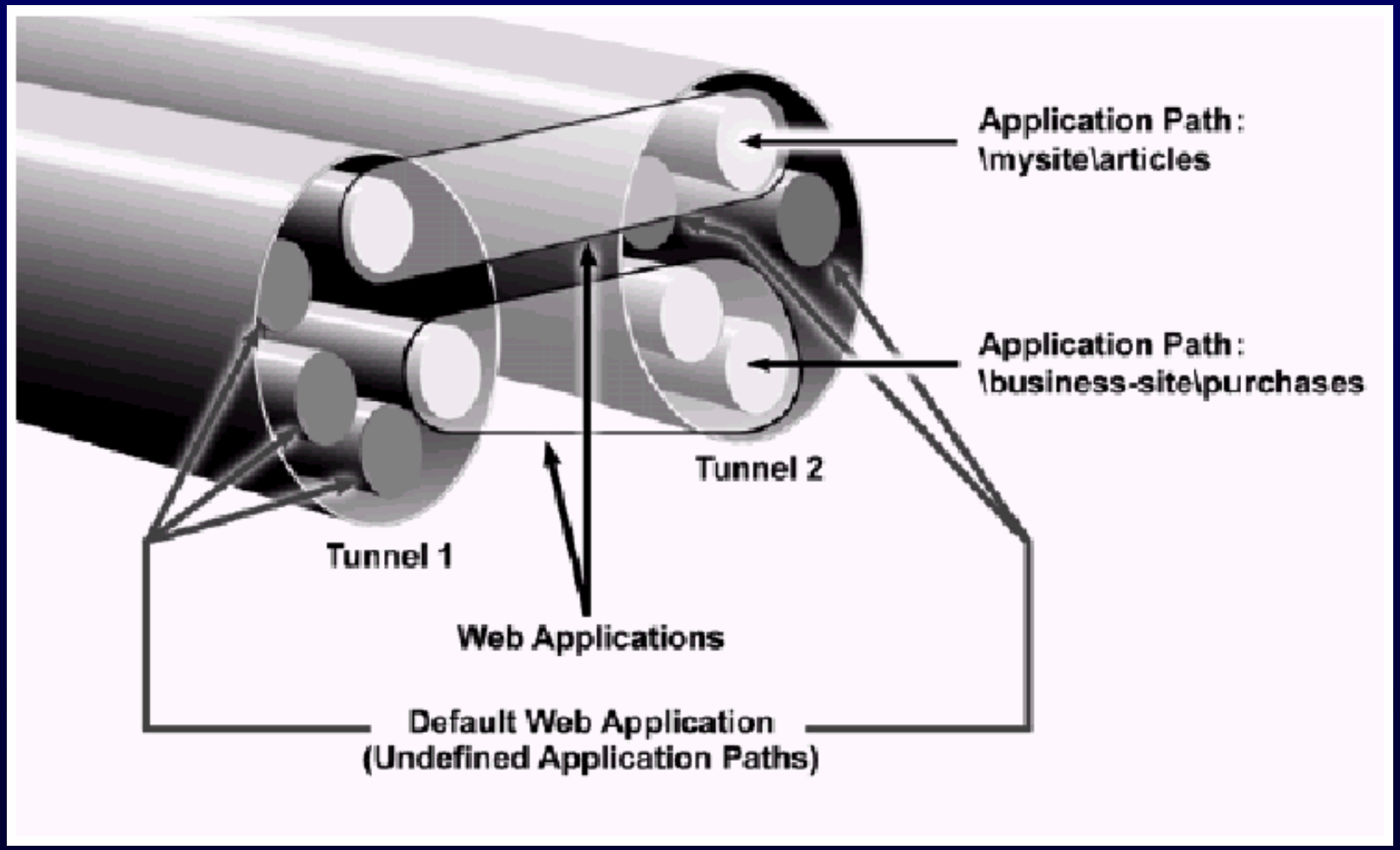
Topologies: Segment unique



Tunnels, Tuyaux et Applications



Tunnels, Tuyaux et Applications



Types de tuyaux

- **Allow List**
  - Pour application hautement sécurisée
  - Créer la liste de toutes les requêtes autorisées:
    - GET /default.htm
    - POST /portfolio/company.cgi
  - Vérification que la requête existe
- **Cookies**
  - Vérifie que chaque « Set-Cookie » envoyé renverra la même valeur sur une requête client.
  - Possibilité d'exclure certains cookies de cette inspection

Types de tuyaux

- **Database**
  - Vérifie les paramètres des requêtes venant du client pour trouver des commandes SQL cachés
    - http://www.XYZ.com/phones/phonelist.cgi?phoneid=34;delete from phones
  - Possibilité d'exclure certains paramètres de cette inspection
- **Logging**
  - Enregistre soit l'en-tête soit le corps de toutes les requêtes et/ou les réponses http passant par InterDo
  - Attention à la taille du Log avec des corps en Unicode

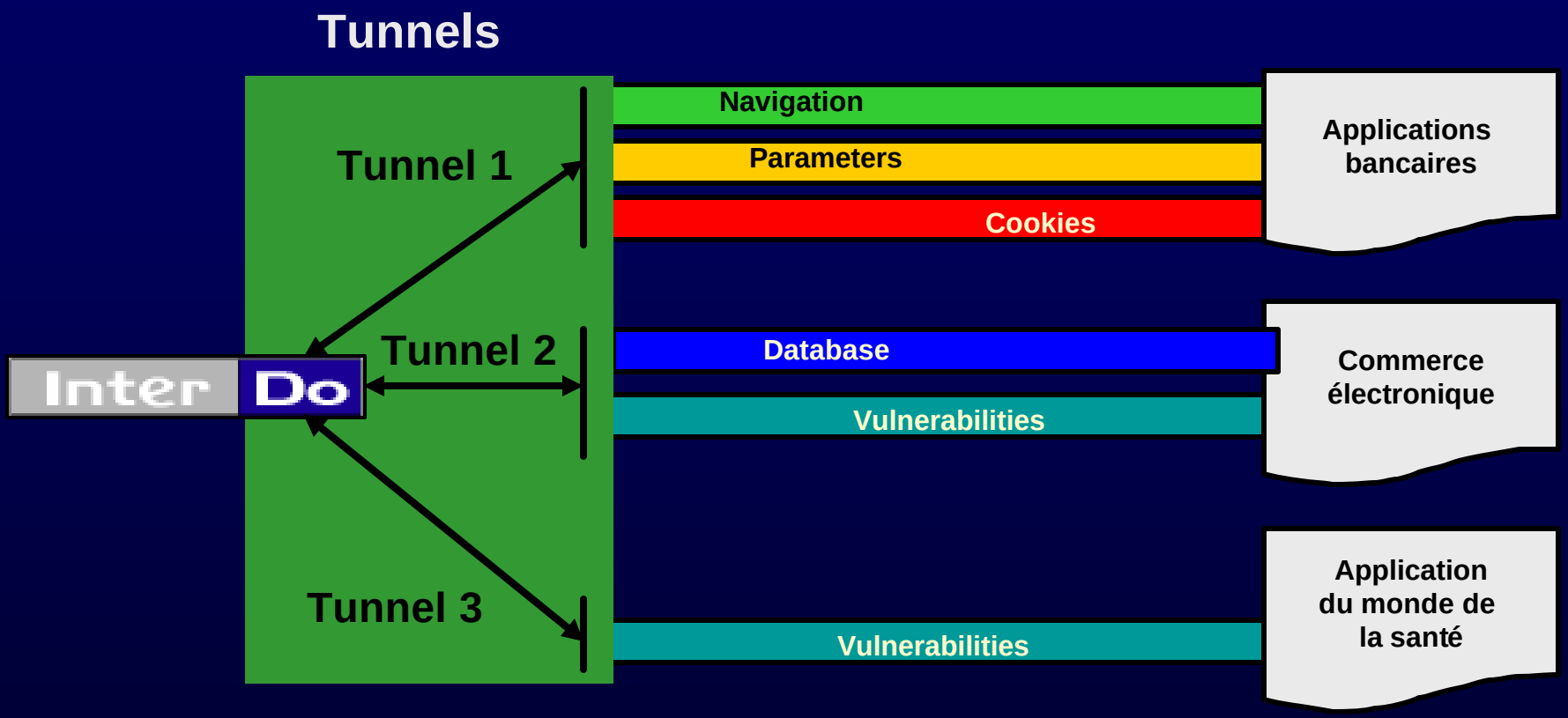
Types de tuyaux

- **Navigation**
  - Vérification que les paramètres contenus dans les requêtes utilisateurs correspondent à ceux envoyés dans la page HTML par exemple dans des HREF
    - HREF=« login.cgi?KnownUser=False »
  - Possibilité d'admettre des valeurs différentes pour certains paramètres
- **Parameters**
  - Vérification que les paramètres contenus dans les requêtes utilisateurs correspondent à une règle définie
    - Book_quantity doit être compris entre 1 et 5
    - GET /myorder.asp? Book_quantity=25 HTTP/1.1
  - Deux modes: Check only ou Allow only

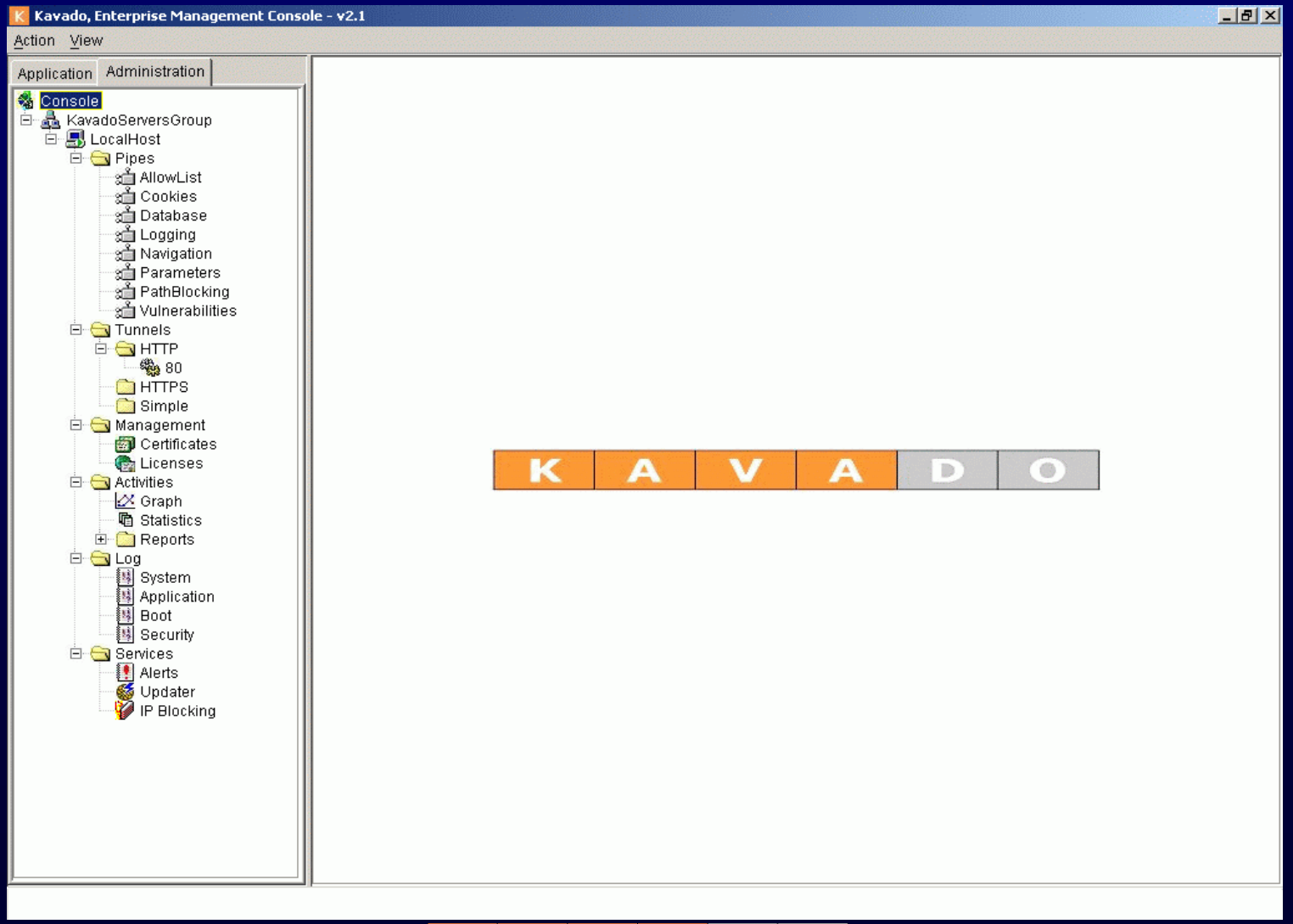
Types de tuyaux

- **Path Blocking**
  - Interdit l'accès à des annuaires virtuels définis
    - /monsite/Clients/special
- **Vulnerabilities**
  - Vérifie la non-existence de vulnérabilités connues
  - Possibilité d'exclure certaines vulnérabilités de cette inspection
  - Possibilité d'ajouter certaines formes de vulnérabilités à cette inspection

Définir les tuyaux nécessaires par applications



Console de Gestion: Vue d'ensemble



Console de Gestion: Surveillance Réseau

Console de Gestion: Journaux

Sécurité

Event type	Date	Time	Reporting object	Reporting resource
Alert	Nov 28, 2001	13:25:27	AllowList	Pipes
Alert	Nov 28, 2001	13:25:27	AllowList	Pipes
Alert	Nov 28, 2001	13:26:23	PathBlocking	Pipes
Alert	Nov 28, 2001	13:27:11	PathBlocking	Pipes
Alert	Nov 28, 2001	13:28:02	Database	Pipes
Alert	Nov 28, 2001	13:28:09	Database	Pipes

Système InterDo

Event type	Date	Time	Reporting object	Reporting resource	Reported object
Warning	Nov 28, 2001	09:59:47	License Manager	Sub Systems	80
Alert	Nov 28, 2001	09:59:47	System Manager	Sub Systems	System Manager
Warning	Nov 28, 2001	12:15:41	License Manager	Sub Systems	80
Warning	Nov 28, 2001	12:21:36	License Manager	Sub Systems	80
Critical	Nov 28, 2001	12:43:36	80	Tunnels	80

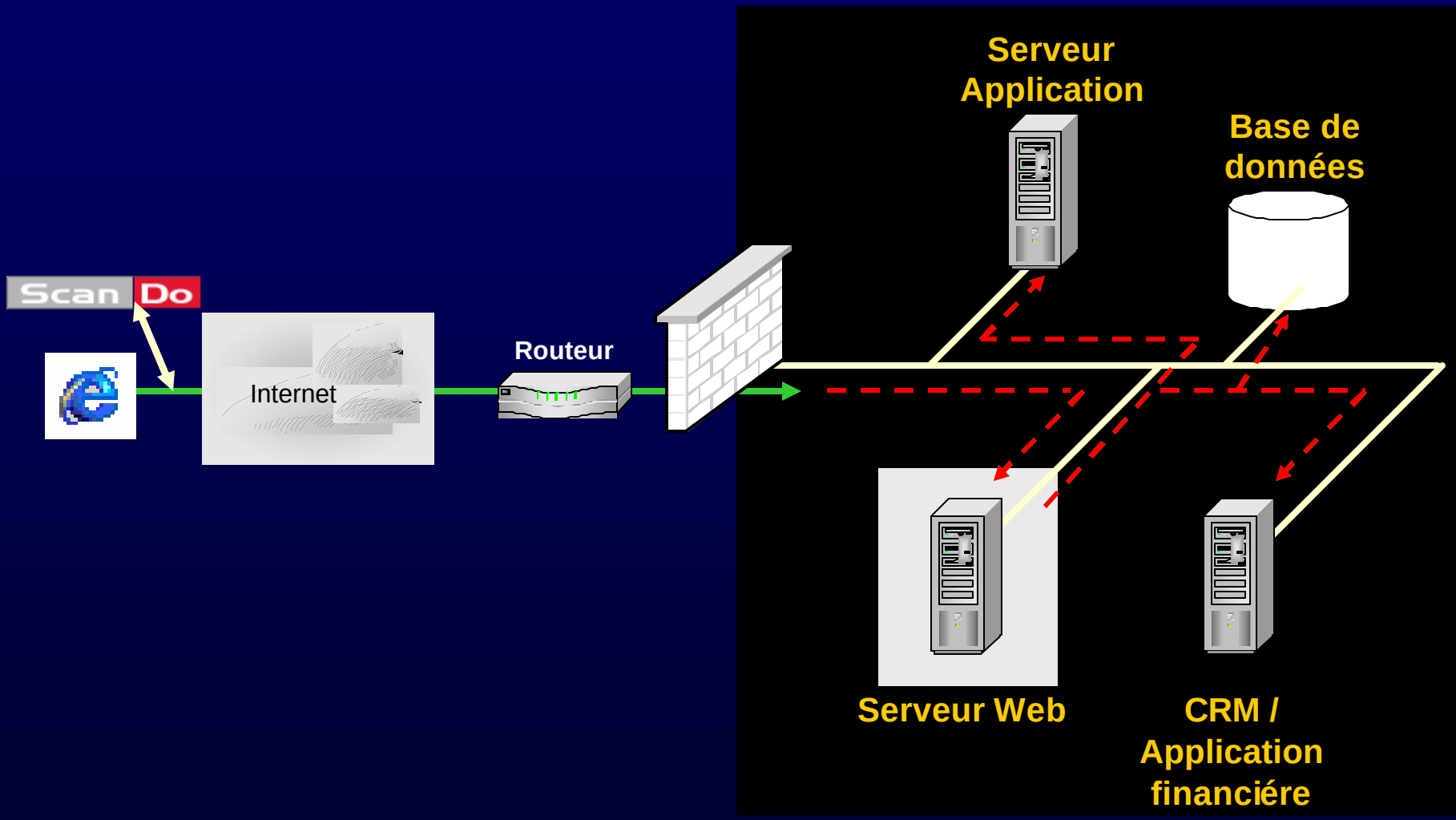
KAVADO

ScanDo™

Analyseur d'Applications Web

Apprentissage-Evaluation et Attaque-Rapport

Comprendre les menaces: ScanDo™



ScanDo™ 1.5 - Apprentissage

Phase d'apprentissage

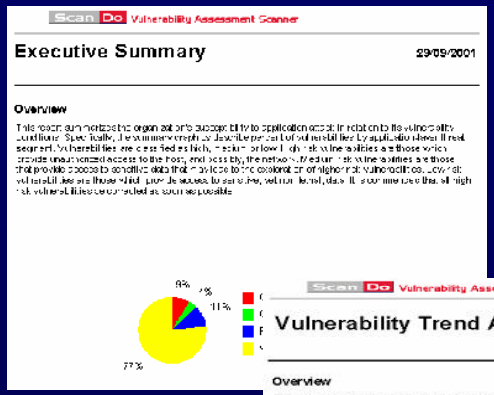
- Interagit complètement avec l'application
  - Effectue le processus en mettant à jour le contexte et la commande de page
- Manipule l'environnement technologique
  - HTML 4.0, gère DOM et cookies , Exécute les scripts, les Flash
- Simule un utilisateur
  - Clique sur les éléments, remplit les formulaires
- Contrôle les erreurs typiques de développement
  - Commentaires, validations des champs d'entrées
- Utilise les technologies PKI
  - SSL avec ou sans authentification mutuelle
- Remplissage automatique des formulaires
  - Avec personnalisations et adaptations

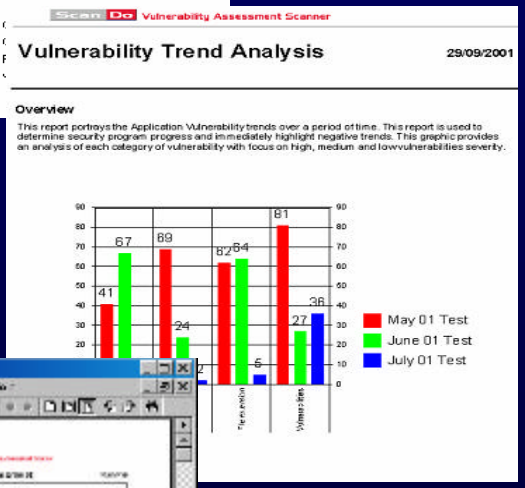
ScanDo™ 1.5 – Evaluation et Attaque

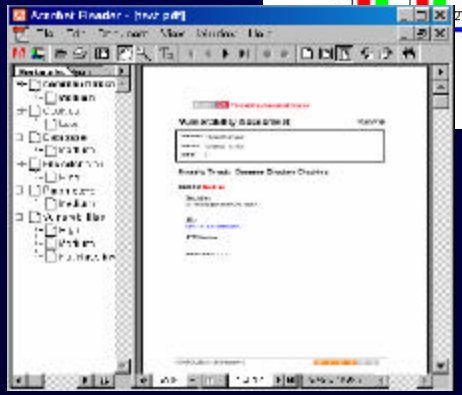
- **Methodologie d'évaluation et d'attaque**
  - Cookie empoisonné
  - Manipulation des paramètres
  - Menaces sur les bases de données
  - Vulnérabilités futées
  - Erreurs de développement
  - Backdoors & erreurs de configurations
- **Scripts Clients d'évaluation et d'attaque**
  - VBScripts, Jscripts
- **API**
  - Architecture ouverte
  - Menaces futures

ScanDo™ 1.5 –Rapports

- Synthèse pour la direction
- Rapports des attaques et évaluation
  - BugTrack, CVE ID;s
- Analyse de tendance
  - Comparaisons avec les résultats précédents
- Formats multiples
  - Texte, PDF, HTML
- Exportation des données
  - XML
- Personnalisation
  - Apparence
  - Contenu
  - Graphiques







ScanDo™ détecte

Analyseur de vulnérabilités

Protocoles

- HTTP 1.1, HTTPS 1.1

Contenu

- HTML 3.2 – 4.0, Flash, JScript, VBScript

Rapports

- Menaces, Recommendations

Yves LE ROUX

KaVaDo France
18, rue de la Procession
75015 Paris
France

Tel: 33 (0)1 43 06 69 90
Email: yves.leroux@kavado.com