



HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

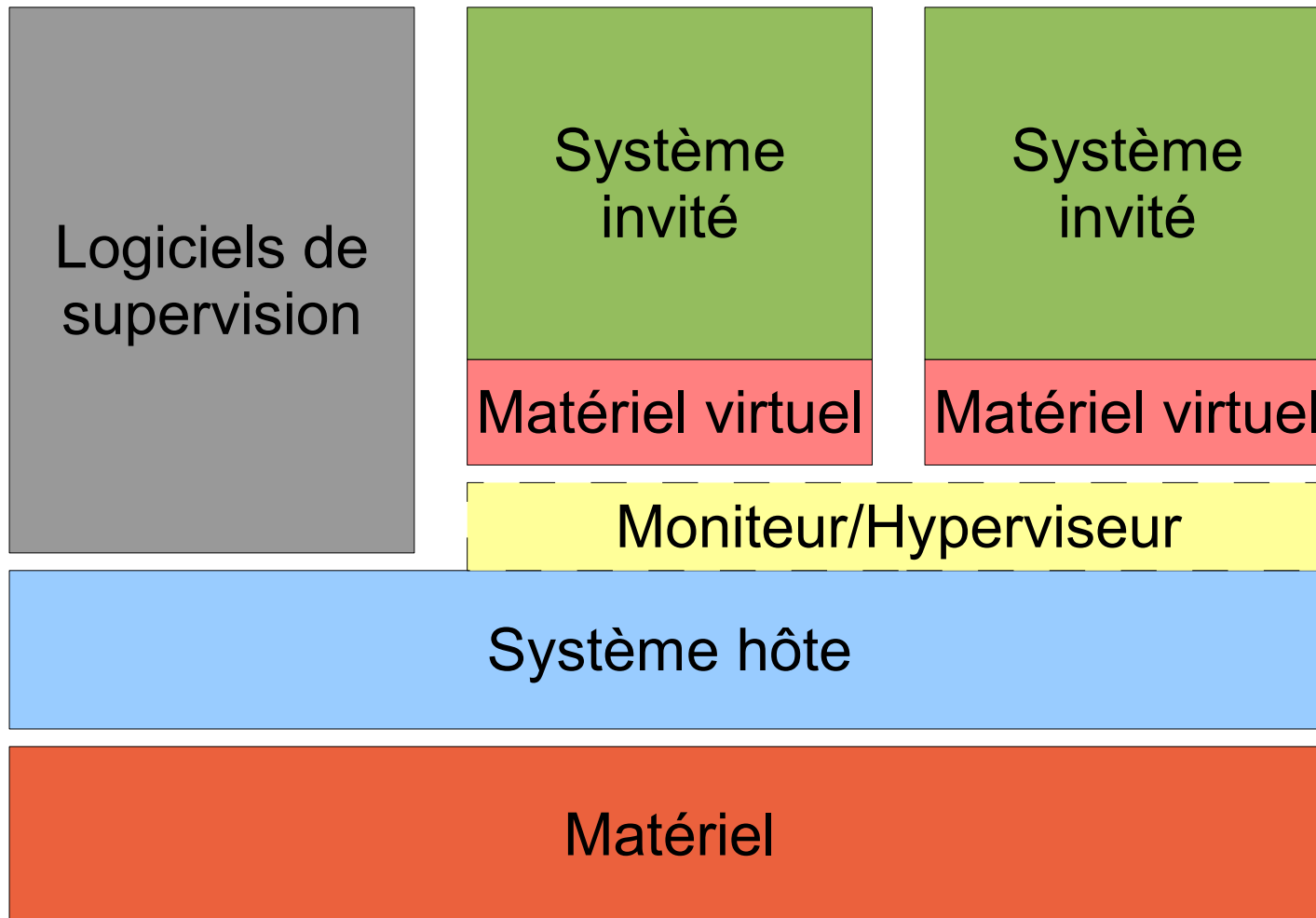
CIO - LMI

Virtualisation et Sécurité

Alain Thivillon
<Alain.Thivillon@hsc.fr>

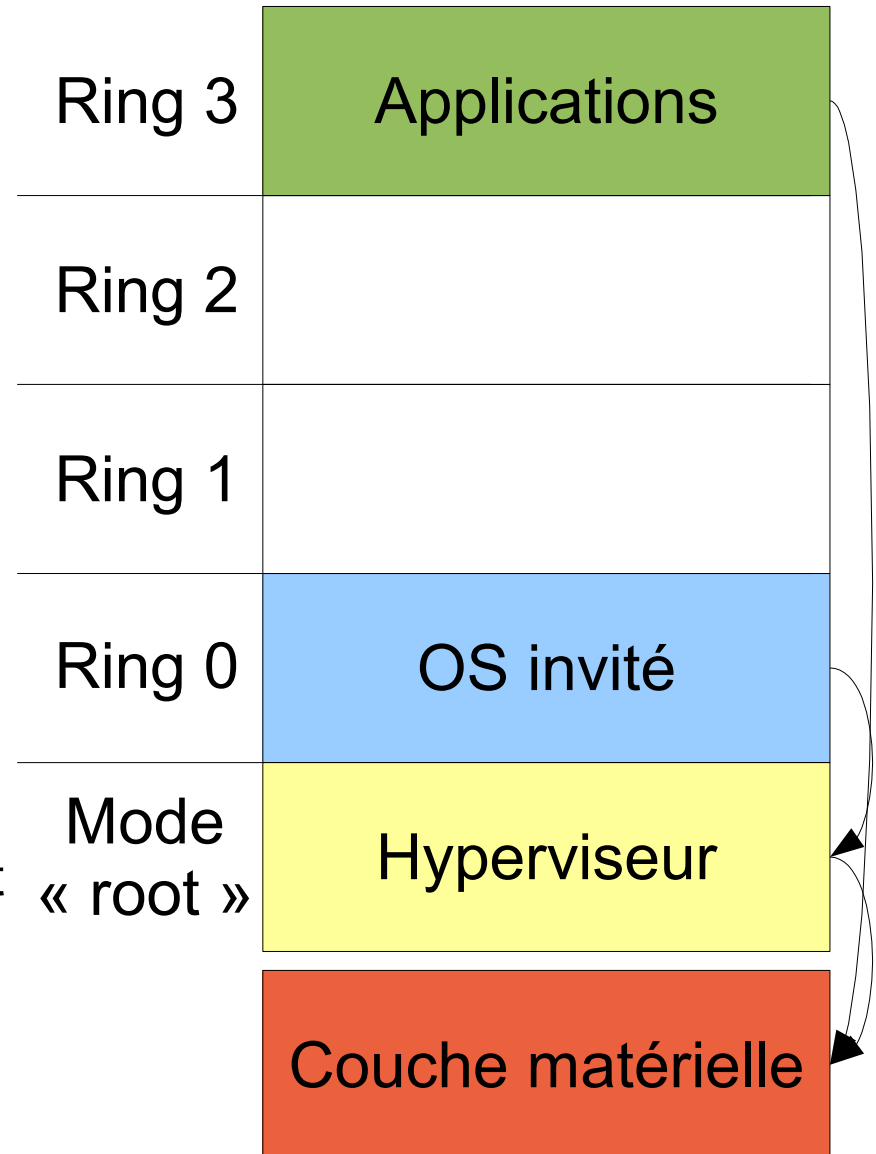
- Société indépendante de conseil en sécurité informatique
 - Depuis 1989
 - <http://www.hsc.fr/>
 - support@hsc.fr
- 16 ingénieurs/consultants
- Domaine d'expertise :
 - Audits de sécurité : système, code, architecture
 - Tests d'intrusion
 - Sécurité organisationnelle (/ISO-2700[1-5]/)
 - Formations techniques et organisationnelles

- Différents types de prestations autour de la virtualisation
 - Audits architecture VMware
 - Audits Firewalls et réseaux virtualisés
 - Audits SAN
 - Étude sécurisation VMware ESX
 - Guide de paramétrage
 - Conseil en architecture
 - Recherche et exploitation de failles dans VMware
 - Tests d'intrusion sanglants
 - Exemple: accès à une console de gestion VMware depuis Internet par rebonds
- Domaines en évolution
 - Attention à la vérité du jour



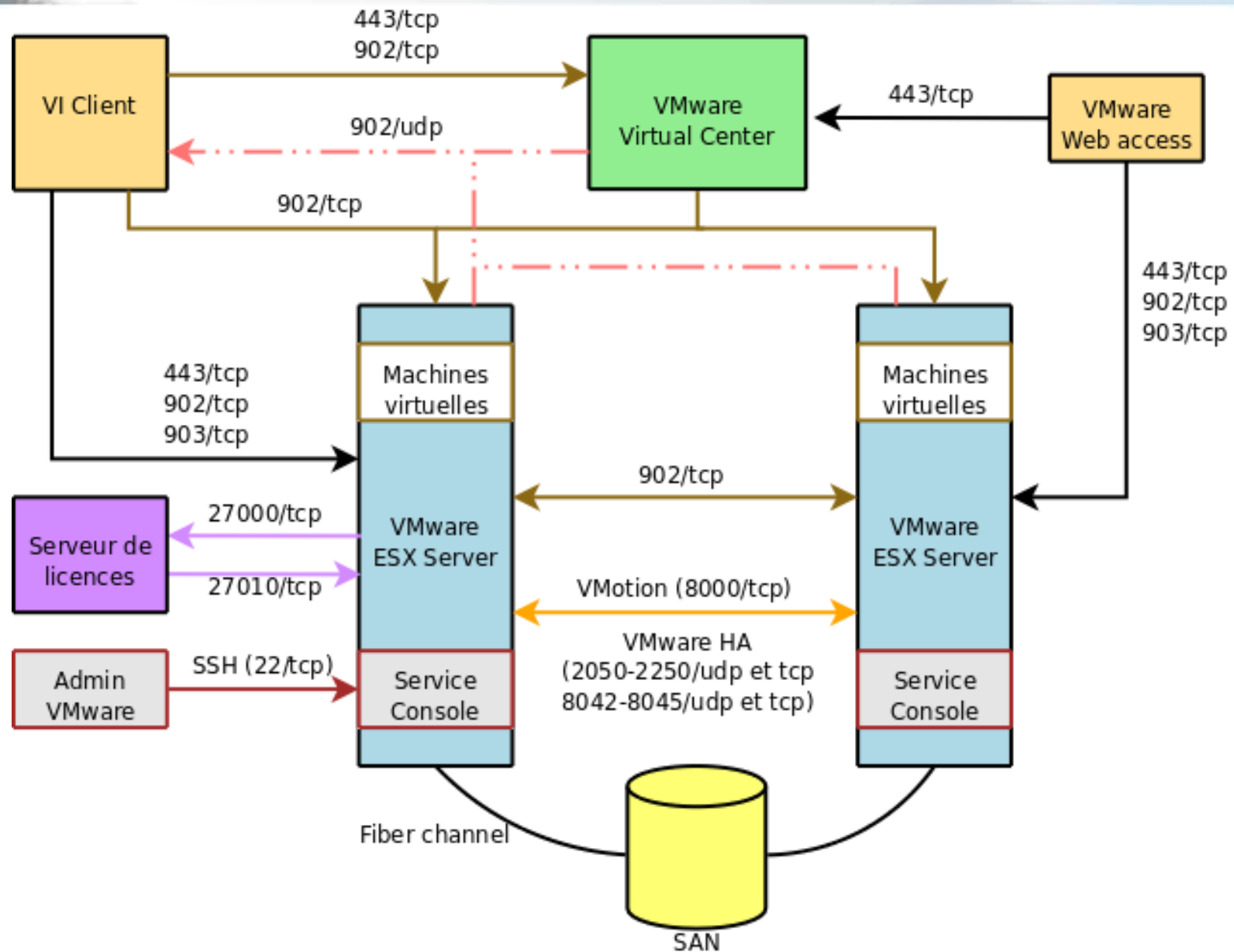
- Vulnérabilités Hyperviseur
 - "Sortir" de l'hyperviseur, exemple accéder à la mémoire d'une autre VM
 - Corrompre le "Virtual Switch"
- Vulnérabilités Périphériques
 - Moyens de communication VM/Hyperviseurs
 - Drivers virtualisés
- Vulnérabilités architecture
 - Ex: Mélange interfaces production/administration/dmz/...
- Vulnérabilités administration
 - Bugs Serveurs Web, Mots de passe, SNMP, ...
 - Exemple IBM HMC mdp par défaut hscroot/abc123
 - Gestion des rôles (ex dev/prod)

- Virtualisation native
 - Applications en Ring 3
 - En Ring 0
 - Système d'exploitation invité NON-modifié
 - Couche de virtualisation tourne « sous » le mode Ring 0
 - Traitement systématique des instructions problématiques par la couche de virtualisation
 - Extensions des processeurs jouent le rôle des hypercalls
 - État des invités stocké dans des structures dédiées du mode racine

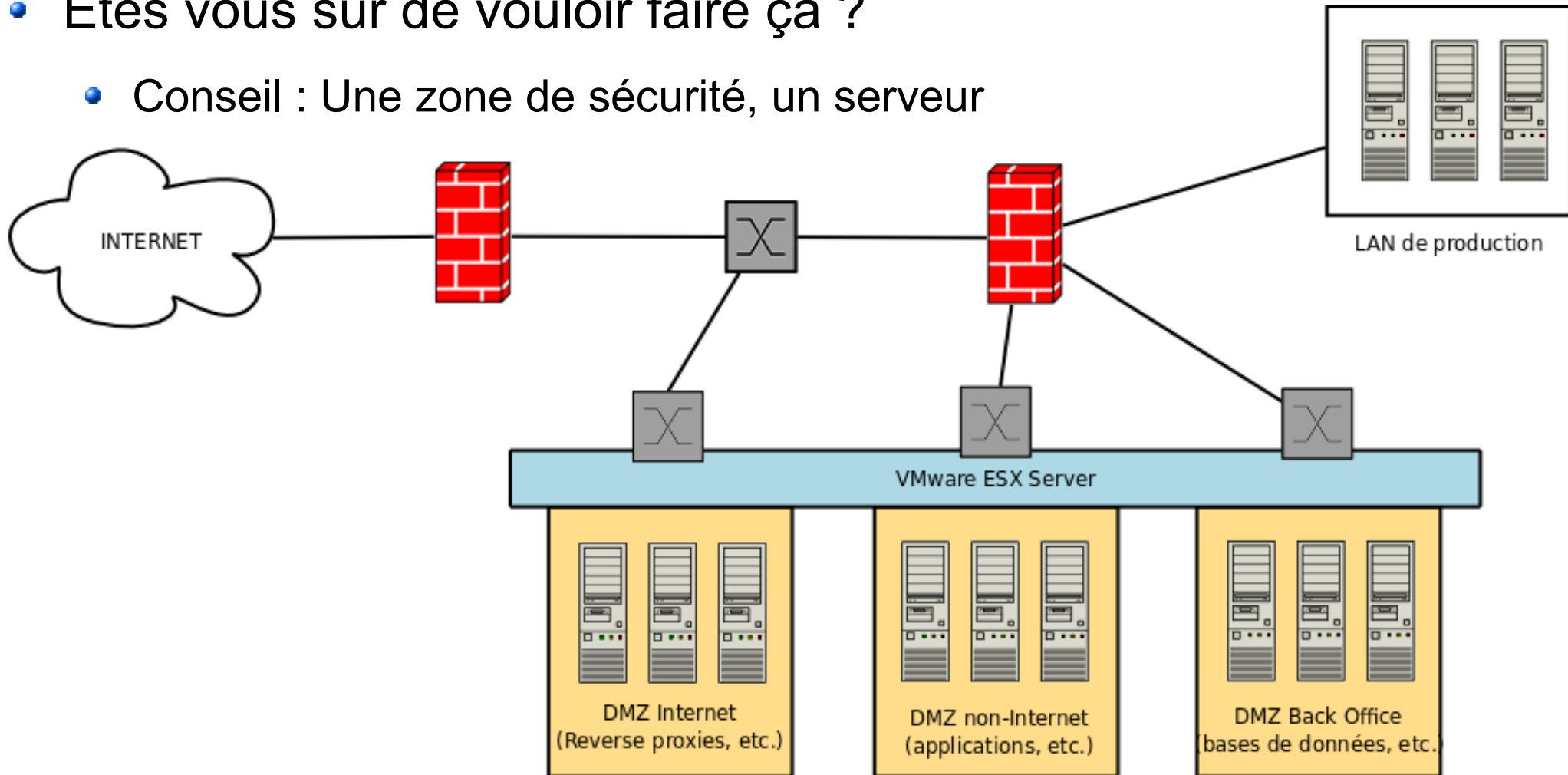


- Une bonne partie de la sécurité repose sur le processeur
 - Nombreux bugs Intel
 - Certains chercheurs en sécurité pensent qu'il est impossible de faire confiance à ce code
- Loïc Duflot (DCSSI) / Joanna Rutkowska (Invisible Things)
 - Utilisation du *System Management Mode* (~Bios, ACPI, ...)
 - Empoisonnement du cache processeur : on écrase la mémoire SMM
 - Exécution de code arbitraire au ring -2
 - Rootkit plus privilégié que l'hyperviseur ...
- D'une manière générale, exploitation pas facile
 - "Attaque gouvernementale"

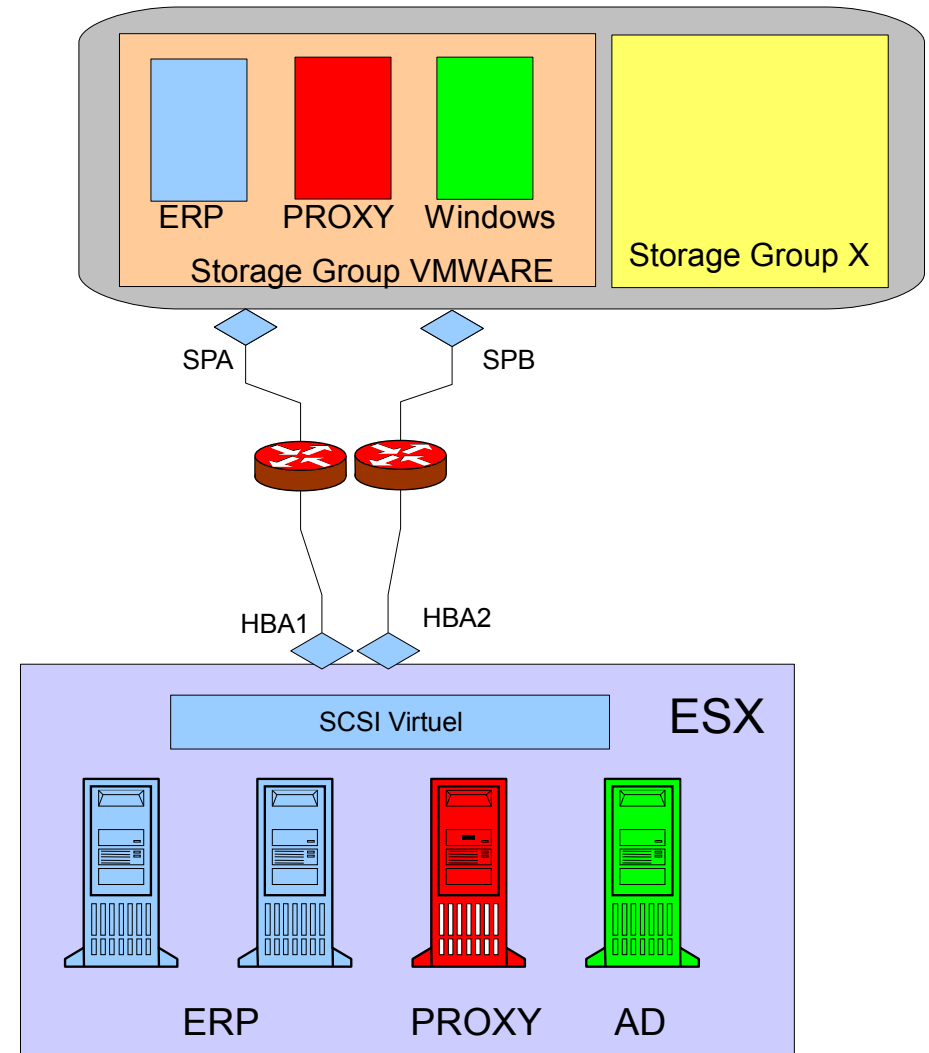
Quelques flux VMware...



- Utilisation du virtual switch de VMware
- Êtes vous sur de vouloir faire ça ?
 - Conseil : Une zone de sécurité, un serveur

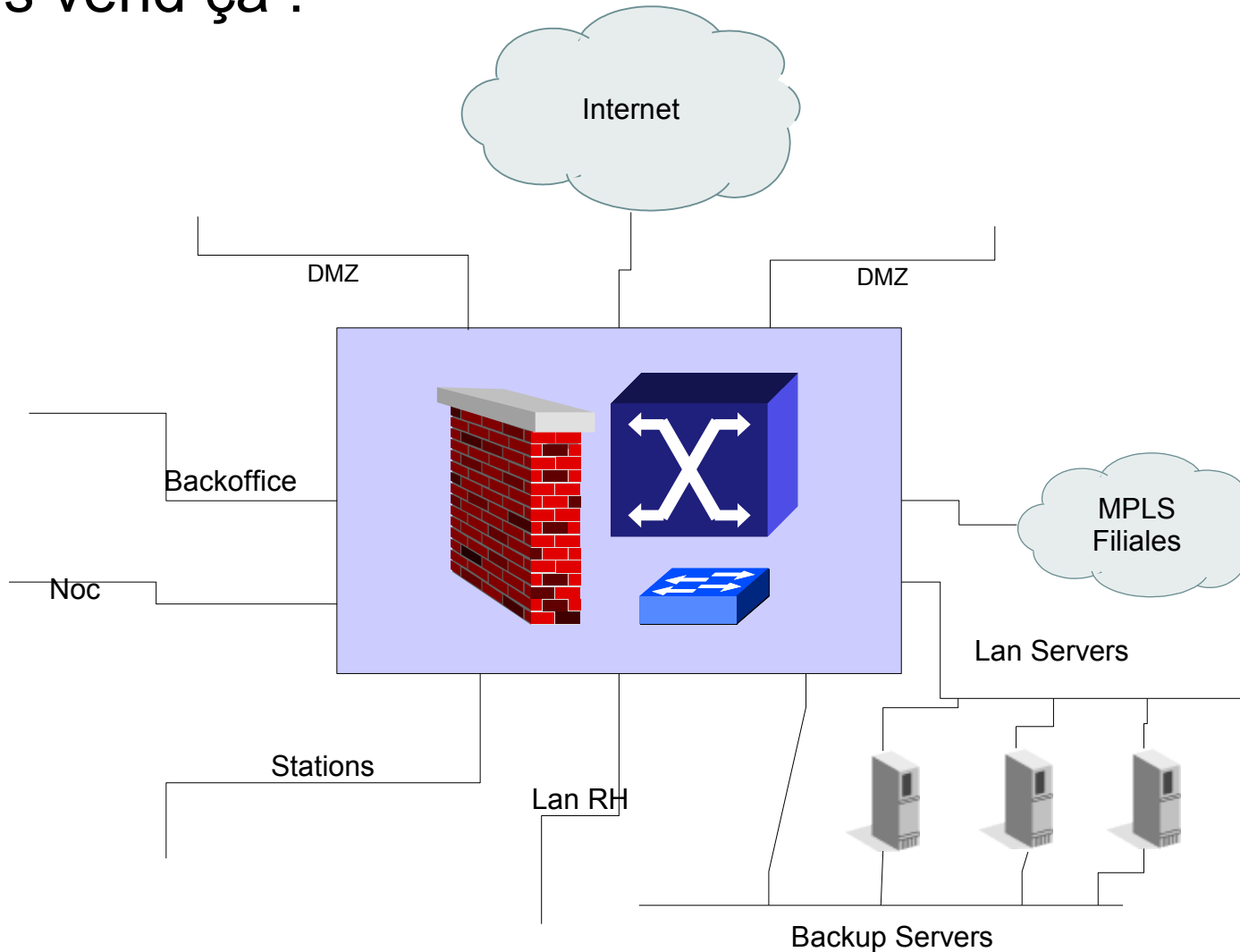


- Le SAN ne voit qu'un seul client
 - Les LUNs sont affectés à chaque VM par ESX
 - On ne peut plus faire de Storage Groupe séparés
 - On ne peut plus faire de Hard Zoning sur les switches
- La encore, on fait confiance à ESX pour effectuer le switching FC
 - Pour des raisons de maintenance, virtualisation des drivers SAN
 - NPIV (Nport ID Virtualization)

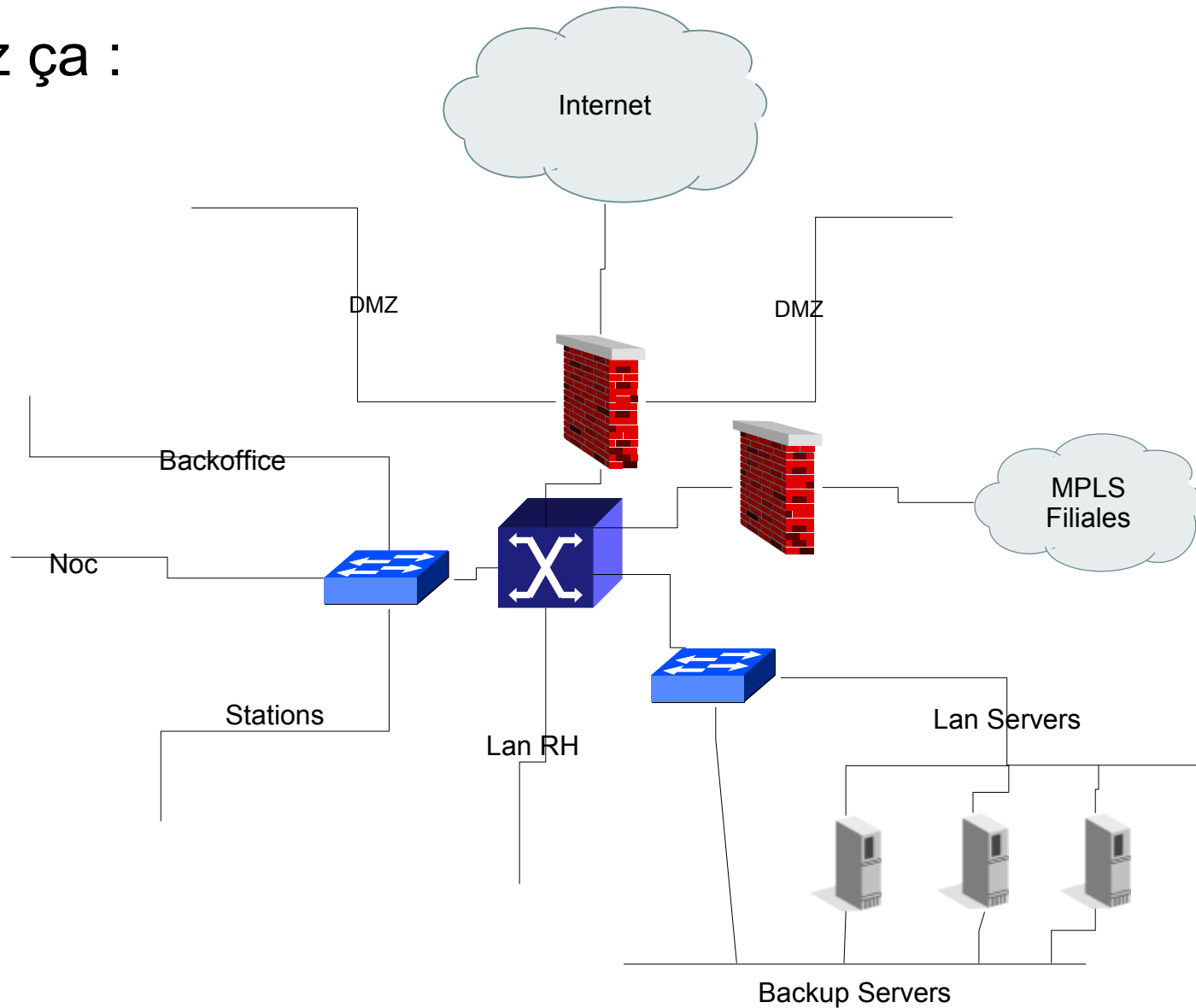


- Virtual Lan : virtualiser le niveau 2
 - Plusieurs LANs sur le même média
 - Transporter les LANs entre les sites
- Virtual Router (VRF chez Cisco)
 - Avoir plusieurs plans de routage séparés dans un seul routeur
 - Utilisé massivement dans les réseaux MPLS (Routeurs PE)
- Virtual Firewall
 - Plusieurs plans de filtrage dans le même équipement, avec politiques de sécurité distinctes
 - Peut être évidemment couplé avec Commutation/Routage/Load Balancing ...
 - Définition d'un "contexte" système + contextes de filtrage

- On vous vend ça :



- Vous avez ça :



Virtualisation : amie ou ennemie pour la Sécurité des SI?

- Détérioré-t-elle la sécurité ?
 - Si mal maîtrisée oui :
 - Vocabulaire complexe et trompeur
 - Architecture difficile à mettre en place (nombreux flux supplémentaires)
 - Demande des compétences
 - L'ajout d'une couche ajoute forcément des vulnérabilités
 - Mélange des rôles (admin Hôtes/admin Guest)
 - Multiplication des serveurs
 - On a déjà du mal à appliquer des patches MS, alors appliquer des patches VMWare sur un système de 40 VM , quel admin va faire ça ...
- Améliore-t-elle ?
 - Bof bof, au mieux c'est neutre d'un point de vue sécurité logique
 - Gros fantasmes de la sécurité dans l'hyperviseur ...

- Faites vous expliquer ce qu'on vous propose
 - Demandez des schémas (ex IP niveau 3), des explications, des docs techniques, des "comment ça marche"
 - La réalité logique doit être clairement affichée
 - On a déjà du mal à penser en 3D, alors en 4 ...
- On ne peut pas virtualiser :
 - Les compétences
 - La sécurité
 - L'administration
- Ayez au moins une personne qui comprend tout
 - Un architecte ou un expert sécurité !

