



HERVÉ SCHAUER CONSULTANTS

Cabinet de Consultants en Sécurité Informatique depuis 1989

Spécialisé sur Unix, Windows, TCP/IP et Internet

**Espace RSSI du CLUSIF**

**4 février 2009**

**Virtualisation et sécurité**

**Julien Raeis** <Julien.Raeis@hsc.fr>

**Nicolas Collignon** <Nicolas.Collignon@hsc.fr>

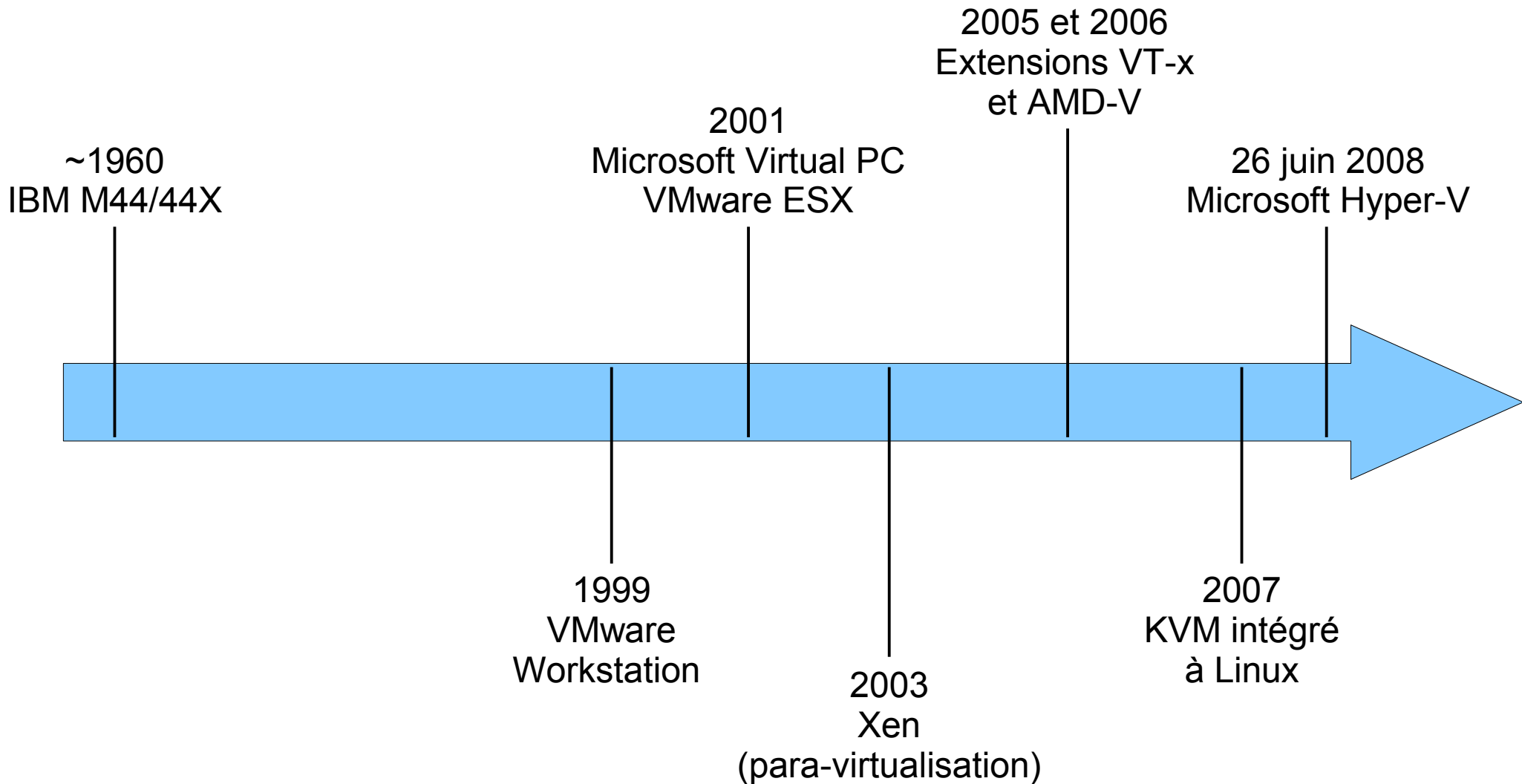
- Rappels sur la virtualisation
- Mesures de sécurité intégrées à VMware
- Revue des vulnérabilités
- Virtualisation et DMZ
- Retour d'expérience HSC
- Conclusion

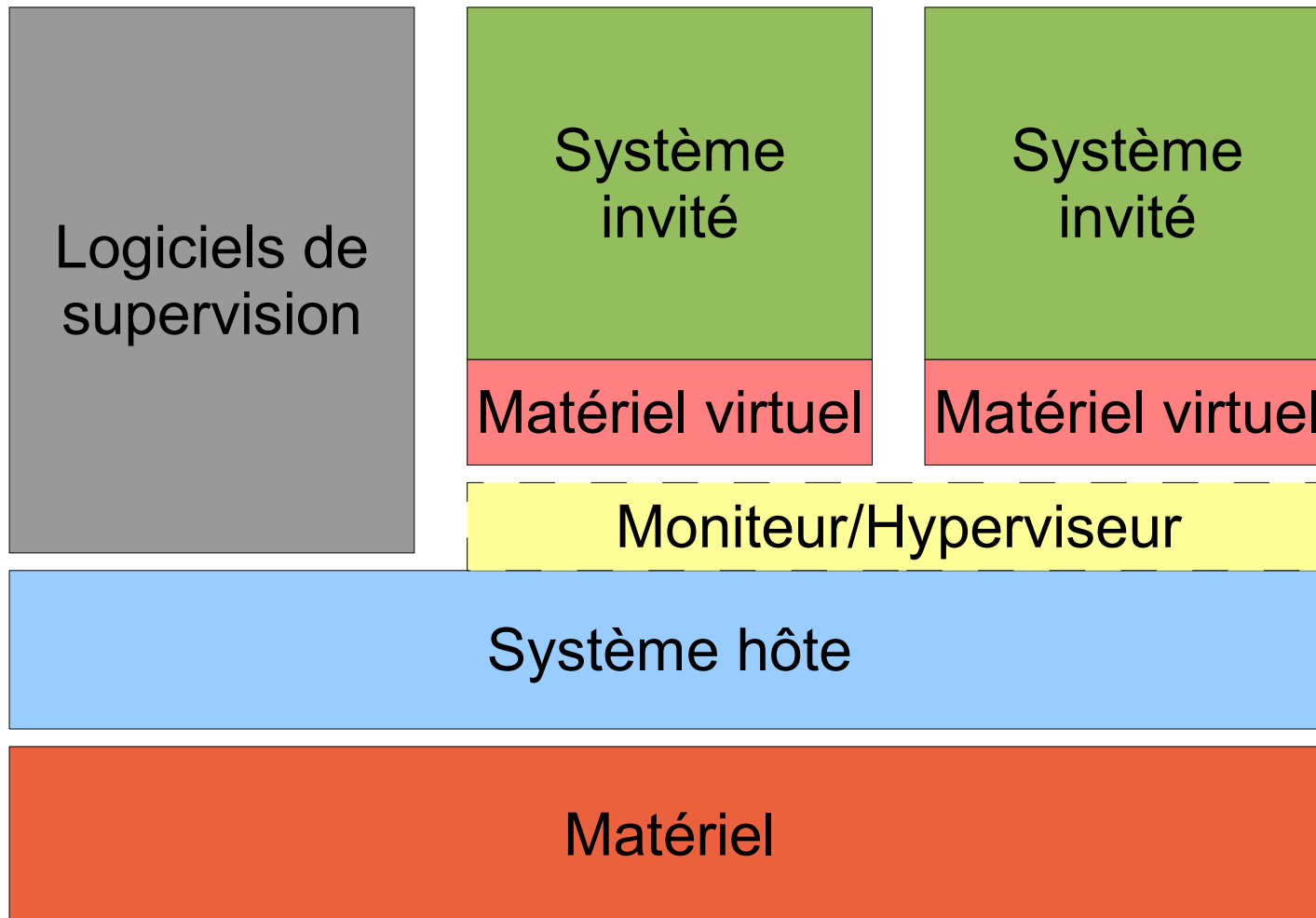
# Rappels sur la virtualisation

- « Virtuel : Se dit des éléments (terminaux, mémoire...) d'un système informatique considérés comme ayant des propriétés différentes de leurs caractéristiques physiques » - *Grand Dictionnaire Encyclopédique Larousse*
- « Virtualisation : abstraction des ressources d'un système informatique. »

- Concept introduit dans les années 60
  - But : partitionner les ressources des coûteux *mainframes* de l'époque
  - IBM M44/44X, naissance du terme « pseudo-machine »
    - Première implémentation de machines virtuelles
  - IBM CP-40
    - Système tournant sur S/360-40
- Perte d'intérêt dans les années 80
  - Déport des applications sur des clients et serveurs x86
    - Architecture « bon marché »
  - Mais coûts d'infrastructure physique élevés, manque de protection en cas de panne, maintenance des postes de travail coûteuse, etc.

- Problème
  - Architecture non-prévue pour la virtualisation
  - 17 instructions ne peuvent être virtualisées simplement
- 1999 : VMware propose une solution
  - Interception (« trap ») et conversion de ces instructions
  - Exécution directe des autres instructions par le processeur





- Au moins 7 types différents !
  - Émulation
  - Virtualisation partielle
  - Virtualisation complète
  - Para-virtualisation
  - Virtualisation native (ou assistée matériellement)
  - Virtualisation par zones
  - Virtualisation applicative
  - etc.

- Émulation
  - Simulation intégrale du matériel
  - QEMU, PearPC, Bochs
  - Principe des émulateurs des vieux ordinateurs/console de jeu
    - Amiga, Atari, etc.
- Virtualisation partielle
  - Partage de ressources matérielles par abstraction
  - Implémentation répandue
    - Adressage virtuel des processus
    - Linux, Windows, etc.

- Virtualisation complète (*Full virtualization*)
  - Systèmes invités tels quels
  - « Emulation » du matériel virtuel
  - VMware Workstation, VMware Server, Virtual PC, etc.
- Para-virtualisation et virtualisation assistée matériellement
  - Quelques contraintes
    - Para-virtualisation nécessite « l'aide » du système invité
    - Virtualisation assistée demande du matériel spécifique (aujourd'hui répandu)
  - Hyper-V, ESX/ESXi, Xen

## Mesures de sécurité intégrées à VMware

- Deux types de produits pour virtualiser
  - Hébergés (« hosted »)
    - VMware Workstation, Server, Player, Fusion
    - Moniteur de machines virtuelles tourne sur l'OS hôte
  - Hyperviseur
    - VMware ESX et ESXi
    - « VMKernel » pour le rapport avec le matériel et la virtualisation
    - Système Linux pour le charger en mémoire, ensuite virtualisé
- Produits d'administration de la virtualisation
  - « Service Console » intégrée au système hôte d'ESX
  - VMware Virtual Center / VMware Infrastructure Client
  - VMware VMotion, HA, etc.

- Authentification et contrôle d'accès
  - Mécanismes intégrés pour VMware Server et ESX sous Linux
  - Interfaçage possible avec Active Directory
- Communications chiffrées
  - Entre VMware Infrastructure Client/Server Console et le serveur
- Isolation entre hôte et invités
  - Par l'hyperviseur, au niveau système et réseau (virtuel, bien sûr)
- Bientôt : VMSafe
  - On agit directement avec l'hyperviseur !
  - Prochaine version d'ESX
  - Tellement sûr que VMware demande un NDA pour avoir des infos

- Options de configuration (pas toujours) documentées
  - <http://sanbarrow.com/vmx.html>
  - Notamment, pour la sécurisation :

```
isolation.tools.copy.enable = FALSE      # Copier
isolation.tools.paste.enable = FALSE     # Coller
isolation.tools.hgfs.disable = TRUE      # Dossiers partagés
isolation.tools.dnd.disable = TRUE      # Drag'n'Drop
...
```

- Restrictions d'authentification par PAM

```
##%PAM-1.0
auth    required      pam_unix.so shadow nullok
account required      pam_listfile.so item=group sense=allow
        file=/etc/vmware/vmwaregroup onerr=fail
account required      pam_unix.so
```

- *Service console* de VMware ESX
  - Pare-feu par l'outil « esxcfg-firewall »
  - MAIS ! Interdiction de rajouter des règles manuellement sous peine de perdre le support VMware
- Autres mécanismes d'ESX
  - Activation ou désactivation de protections matérielles sur les processeurs (NX, Hyper-Threading, etc.)
  - Système de rôles (type RBAC) pour les utilisateurs de Virtual Center
  - Protections réseau niveau 2
    - Segmentation réseau par VLANs (sur les commutateurs virtuels par exemple)

- Déploiement manuel
  - Pour les produits VMware
    - ESX : simples « patches »
      - Demandent parfois de redémarrer complètement le système hôte !
    - Virtualisation hébergée : réinstallation complète
  - Pour les machines virtuelles
    - Chaque machine est responsable de sa mise à jour
    - Canaux classiques (Windows Update, Red Hat Network, etc.)
- Automatisation possible depuis Virtual Center 2.5
  - Même dans les systèmes invités en utilisant un protocole de communication interne à VMware

- Tout ou presque repose sur la sécurité de Windows
  - Authentification
  - Autorisations
  - Permissions sur les systèmes de fichiers (« partitions »)
  - Pare-feu de Windows
- Tout comme VMware...
  - Isolation entre les machines virtuelles et l'hôte
  - Système « parent » (hôte) doit être isolé et administré séparément
  - Restrictions au niveau processeur

# Revue des vulnérabilités

- Diffusion de correctifs de sécurité
  - De 2003 à 2005
    - Pas de « centre de sécurité VMware »
    - 10 vulnérabilités corrigées
  - Puis mise en place d'un système d'alertes et d'avis
    - 2006 : 10 avis pour 17 vulnérabilités
    - 2007 : 6 avis pour 25 vulnérabilités
    - 2008 : 19 avis pour pour 49 vulnérabilités
    - 2009 : 1 avis pour 3 vulnérabilités
- Avis touchent à la fois
  - Les produits VMware
  - Les paquets tiers (Service Console de ESX Server)

Année	Total	ESX	Virtualisation hébergée	Produits VMware	Produits tiers	Sortie de l'isolation
2003	3	3	1	0	3	0
2004	6	5	2	3	3	0
2005	2	0	2	2	0	1
2006	17	16	2	7	10	0
2007	25	23	8	8	17	1
2008	49	38	18	15	34	2
2009	3	3	0	1	2	0

- 4 sorties d'isolation
  - Depuis l'invité vers l'hôte
  - 3 nécessitent des conditions particulières, non-présentes par défaut
  - 2 sont uniquement valables sur VMware Workstation et Player
- Quelques élévations de privilèges
  - Dans l'invité avec les VMware Tools notamment
  - Dans l'hôte par des produits tiers

- Diffusion de correctifs de sécurité
  - Pas vraiment de recherche autour de Xen jusqu'en 2006
    - Très peu d'avis... mais pourtant des failles !
  - Patch souvent directement depuis les sources
    - Heureusement les distributeurs suivent rapidement
    - Rachat par Citrix devrait accélérer et formaliser les processus
- Historique des avis (non-officiels)
  - 2006 : 2 avis pour 2 vulnérabilités
  - 2007 : 4 avis pour 7 vulnérabilités
  - 2008 : 6 avis pour 9 vulnérabilités

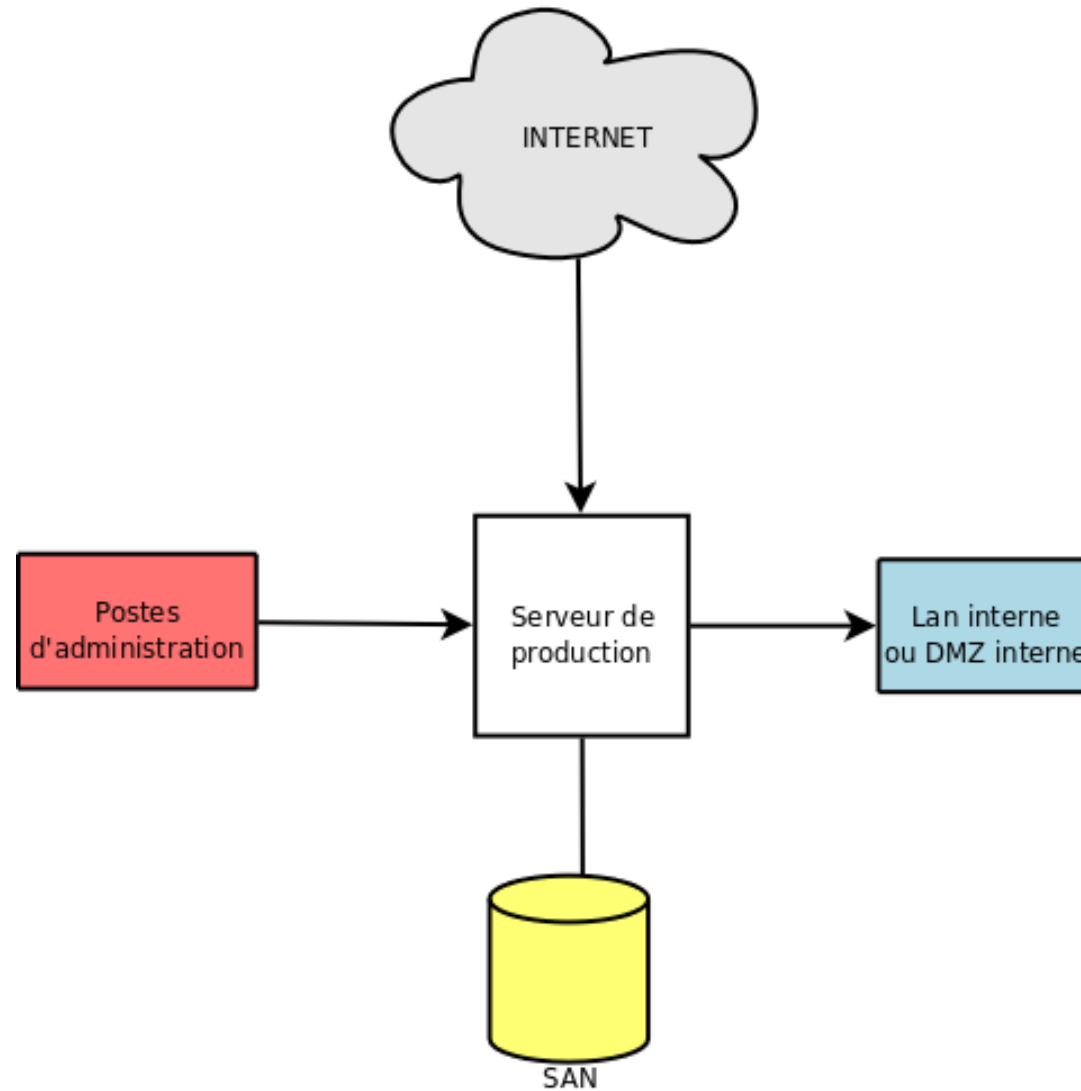
Année	Total	Hyperviseur	Produits tiers	Sortie de l'isolation
2006	2	1	1	0
2007	7	3	4	1
2008	9	5	4	3

- 4 sorties d'isolation
  - Depuis l'invité vers l'hôte ou entre les invités
  - 2 nécessitent des conditions particulières
  - 2 ont été publiquement prouvées et exploitées par des chercheurs
- Quelques élévations de privilèges
  - Dans l'invité
  - Dans l'hôte également

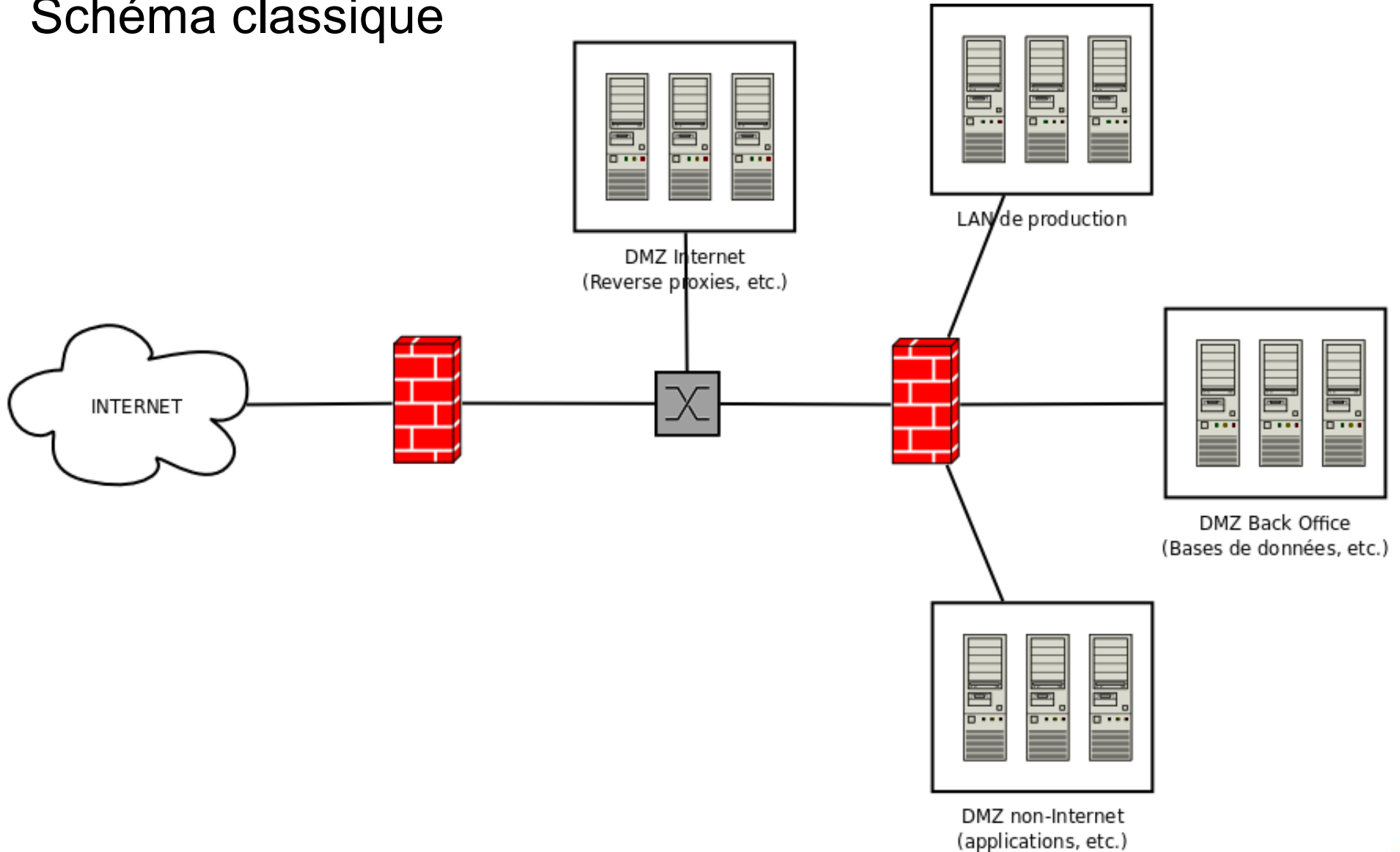
- Pas la moindre vulnérabilité à déplorer... pour l'instant !
  - Produit très jeune (juin 2008)
  - « Extension » de Windows plus qu'un produit à part entière
    - Profite des mécanismes de sécurité de Windows Server 2008
    - Code audité et respectant des *best practices* de développement
  - Les chercheurs en sécurité s'y intéressent de plus en plus...
    - ... on peut espérer quelque chose publiquement en 2009

# Virtualisation en DMZ

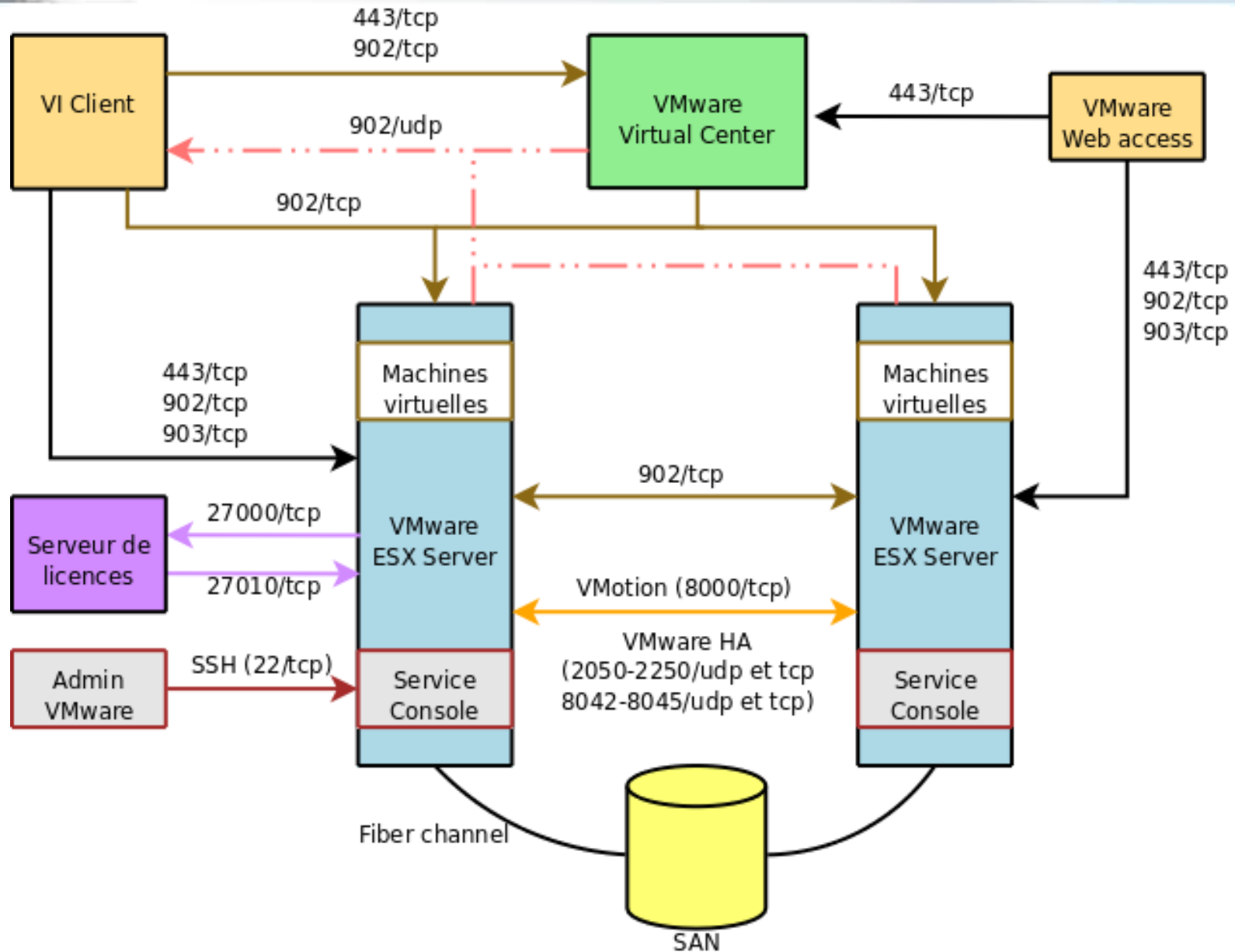
- Virtualisation des serveurs en production
  - Donc en DMZ
- Différences avec un réseau local ?
  - Criticité des données
  - Impératif d'isolation (principe même de la DMZ)
- Des risques supplémentaires
  - Passage de N à au moins N+1 machines (virtuelles ou non)
    - L'administration des systèmes hôte à prendre en compte
    - **!! Système hôte compromis = TOUTES les machines virtuelles compromises !!**
  - Un vrai casse-tête avec les flux réseau et les pare-feu

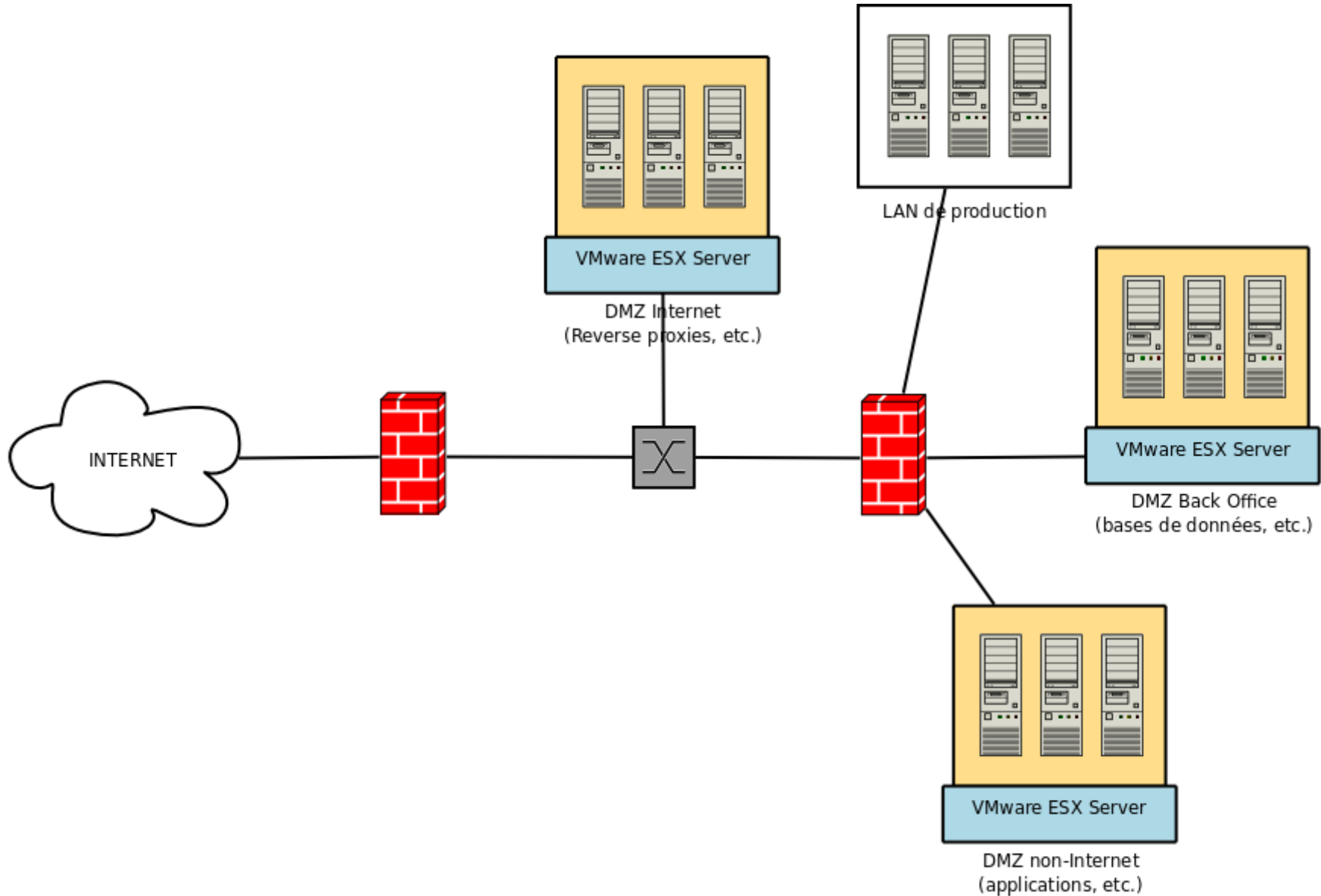


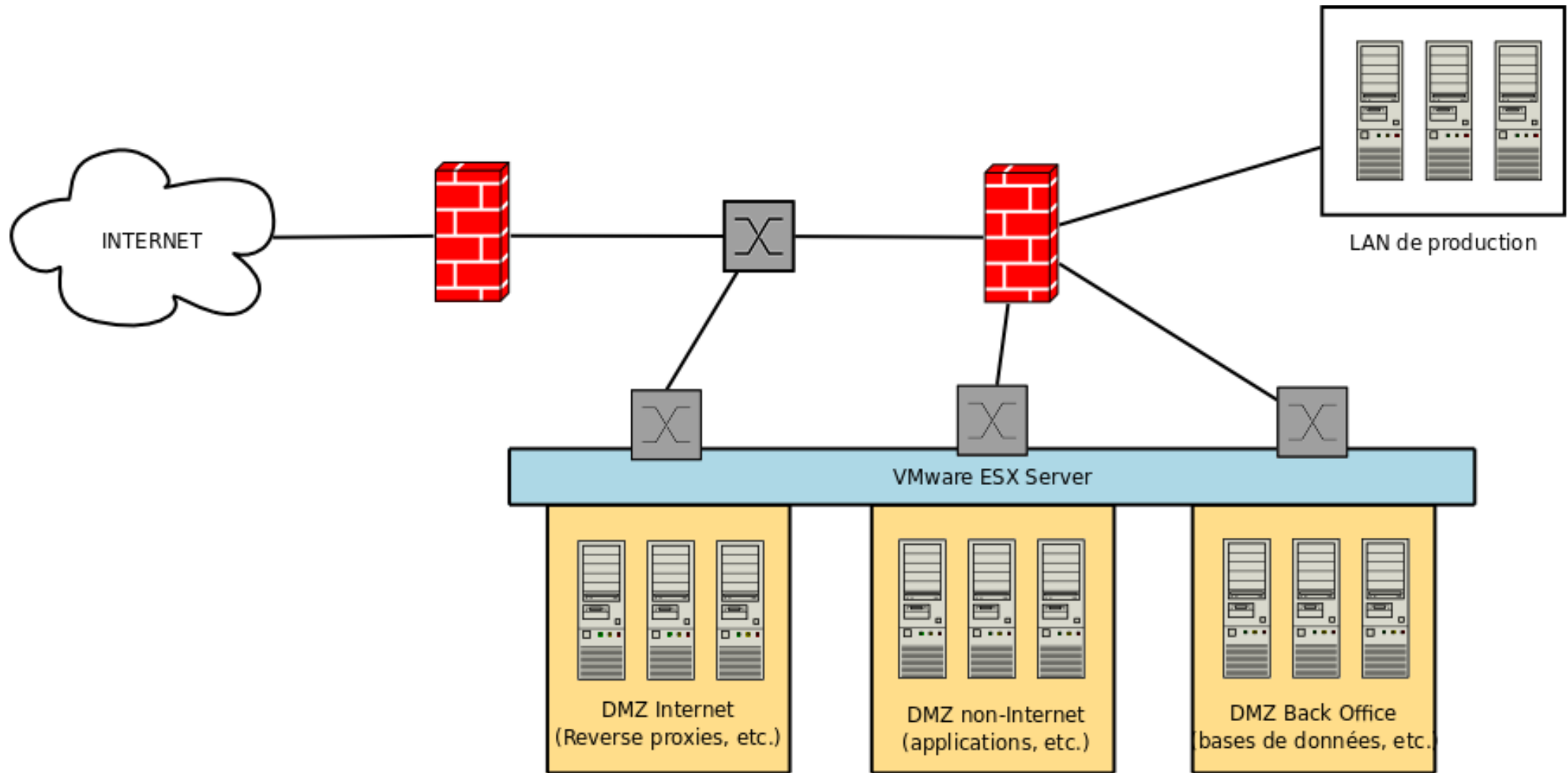
- Schéma classique

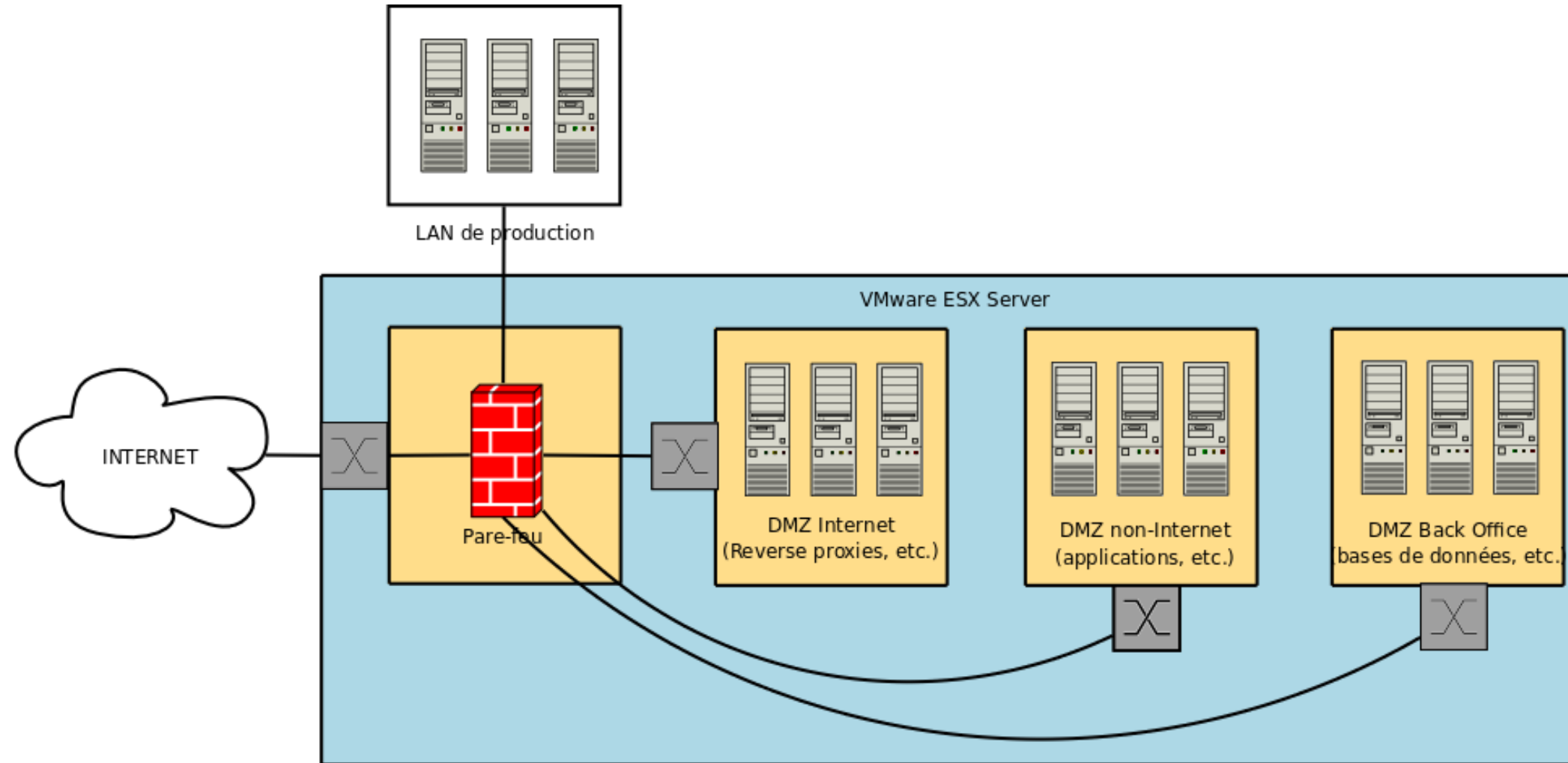


## Quelques flux VMware...









# Retour d'expérience HSC

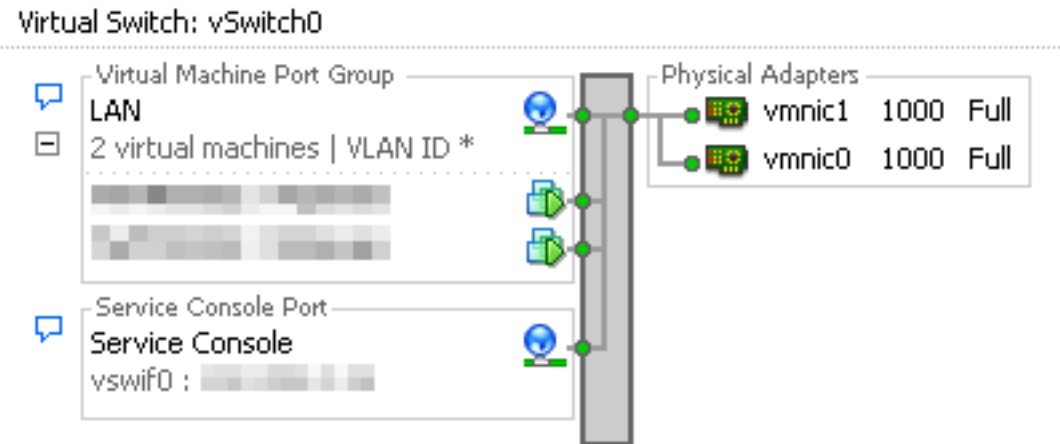
- Audits sur plates-formes de virtualisation
  - ESX Server uniquement
    - ESXi prochainement
  - Audit de configuration
  - Audit d'architecture
    - Intégration de la virtualisation en DMZ
- Travaux de recherche
  - Communications avec l'hyperviseur
  - Protocoles de communication
  - Gestion des sessions
  - Les « Shared Folders »
  - Comment exploiter une vulnérabilité dans l'hyperviseur

- Correctifs de sécurité
  - Réticences à redémarrer les systèmes hôtes...
    - Tous les correctifs ne sont pas forcément déployés
    - Machines virtuelles rarement patchées...
- « Service console »
  - Minimisation des services déployés
    - Outils de supervision désactivés
    - Activation du SNMP
    - Serveur HTTP de gestion désactivé
  - Activation du pare-feu
  - Restriction du service SSH

- VMware Virtual Center
  - Création d'utilisateurs et rôles précis
    - Administrateurs de machines virtuelles (avec droit de redémarrage)
    - Administrateurs ESX (accès à la configuration des VMs)
  - Partage des ressources strict pour éviter les dénis de service
- Systèmes invités
  - Déploiement des VMware Tools (minimisés)
  - Considérés comme des machines physiques
  - Options d'isolation activées
    - Copier/coller, *Drag'n'Drop*, etc.
  - Suppression des périphériques virtuels inutiles

- Séparation stricte de la « Service Console »

Pas bien ! →



Virtual Switch: vSwitch0



Virtual Switch: vSwitch1



← Bien !

- Autres possibilités d'amélioration
  - Pare-feu de périmètre
  - Pare-feu virtuel (cf. partie DMZ)
  - Utilisation de VLANs
    - Dans ce cas, première architecture vue précédemment peut être OK
    - Trois niveaux :
      - Invités
      - Commutateurs virtuels
      - Commutateur physique à la sortie du réseau virtuel
  - Dans tous les cas, filtrer les entrées/sorties de la console de service
    - **Rappel ! Point critique : hôte compromis = architecture compromise**

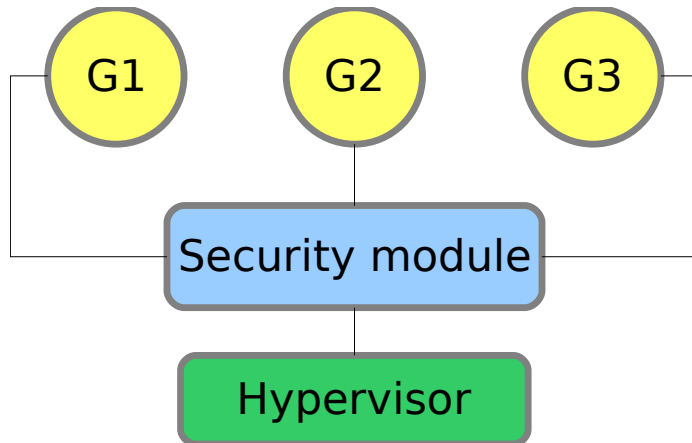
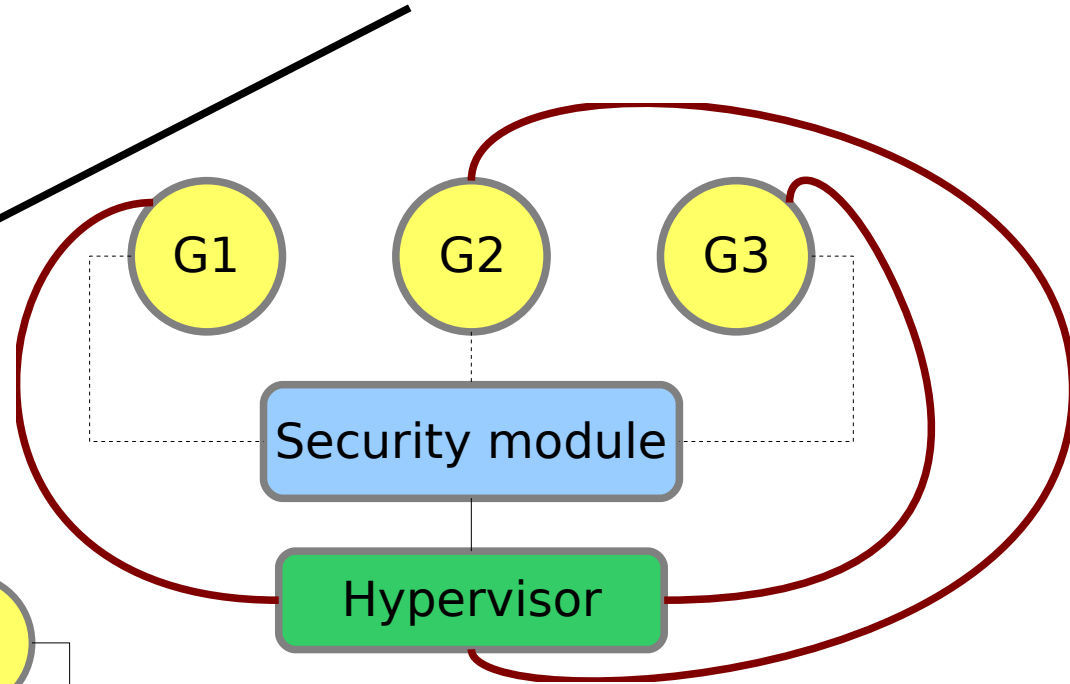
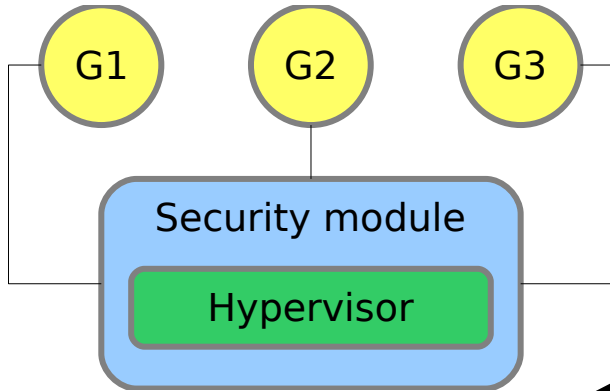
- Système de migration « à chaud » de machines virtuelles
  - En fait, migre essentiellement les processus...
  - ... mais généralement pas les données
- Utilise un canal dédié (cf. schéma de flux)
- Données passent en clair
  - Possibilité d'intercepter au vol une machine virtuelle...
  - ... de la modifier...
  - ... et de la réinjecter dans le nouveau système !
- Quelques travaux de recherche
  - Rien de concret et d'utilisable publiquement encore.

# Conclusion

# 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
- Améliore-t-elle la sécurité ?
  - Pour la disponibilité oui, sans doute
  - Bientôt contrôle de la sécurité des systèmes invités depuis l'hôte
    - Rôle d'anti-virus, HIDS et HIPS intégrés
    - Plus de confiance nécessaire
    - Dans VMsafe bientôt... (ESX 4 ?)
    - ... déjà « vendu » par des sociétés tierces !

# Sécurité de la virtualisation ou virtualisation de la sécurité ?



- <http://www.vmware.com/>
- <http://www.vmware.com/security/>
- <http://communities.vmware.com/>
- <http://www.virtualization.info/>
- <http://chitchat.at.infoseek.co.jp/vmware/backdoor.html>
- <http://sanbarrow.com/>

**Merci de votre attention**  
**Questions ?**

**[Julien.Raeis@hsc.fr](mailto:Julien.Raeis@hsc.fr)**

**[Nicolas.Collignon@hsc.fr](mailto:Nicolas.Collignon@hsc.fr)**

**<http://www.hsc.fr/>**