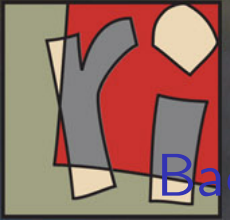
SAFE-OS

Thomas Hérault
Sylvain Peyronnet Sébastien Tixeuil

26 mars 2009



Sommaire

- Background
  - Objectifs du projet
  - L'approche de SAFE-OS
- Description de XEN
  - Architecture
  - Virtualisation du CPU et de la mémoire
  - Gestion des entrées/sorties
- Xen et la sécurité
- SAFE-OS
  - Architecture
  - Partitionnement
  - Affichage - X
  - ssh
  - Firewalling / Configuration réseau
- Gestion du projet
- Distribution
- Évolutions prévues

Objectifs du projet

L'objectif du défi SEC&SI est de *mettre à la disposition des citoyens un système d'exploitation sécurisé permettant d'accéder depuis un ordinateur aux services de banque en ligne, d'e-administration et à un service d'envoi de messages au minimum signés*.

- Ergonomie
- Compatibilité
- Sécurité - confidentialité
- Adaptabilité

L'approche de SAFE-OS

La protection des services (login distant par exemple) est aujourd'hui fréquemment assurée par virtualisation.

- Compartimentage des processus (cover channels)
- Résistance aux DOS
- Autres raisons non liées à la sécurité (équilibrage de charge, maintenabilité, etc.)

SAFE-OS propose d'utiliser les mêmes techniques de virtualisation pour sécuriser le poste de l'internaute.

Notre expertise

- Virtualisation : un outil pour l'étude de performance des machine parallèles (réalisation du framework VDS)
  - Notion de repliement
  - Virtualisation des couches basses du réseau
  - Injection de fautes
- Systèmes répartis : algorithmes tolérants aux fautes byzantines
  - Attaques distribuées et coordonnées
  - Approche masquante / approche non-masquante
  - Attaques transitoires ou systématiques

Choix techniques

- Utilisation de logiciels pré existants intégrés au sein d'une solution innovante
- Xen paravirtualisation (version 3.3 - GPL 2)
- Base du système : debian lenny

Description de XEN

- Approche classique : la couche physique virtuelle est fonctionnellement équivalente à la couche physique réelle
  - Difficile à implanter (x86)
- Approche Xen : il n'y a pas équivalence entre la couche réelle et la couche virtuelle. A la place Xen utilise la paravirtualisation.
- Paravirtualisation : l'OS invité est modifié pour fonctionner en parallèle avec d'autres systèmes modifiés
  - Avantage : performances améliorées
  - Modifier le système peut être difficile

Description de XEN : CPU virtuel

- Les CPUs x86 ont 4 modes d'opérations (ring 0 à ring 3). Ring 0 est celui avec le plus de privilèges, ring 3 celui avec le moins
- Xen opère au ring 0 (place classique du noyau)
- Le noyau est déplacé au ring 1 ou 2. C'est cette étape qui rend nécessaire une modification de l'OS
- L'espace utilisateur est en ring 3, ce qui est classique
- Xen est mappé dans les 64 premiers MO de la mémoire (évite un flush tlb)

Description de XEN : CPU virtuel

- Utilisation de la segmentation pour protéger Xen contre un OS malicieux
- Pour effectuer une opération privilégiée : hypercall vers Xen
- System calls de l'espace utilisateur vers le noyau de l'OS invité directement (vérification du trap handler)

Description de XEN : MMU virtuelle

C'est la tâche la plus difficile pour l'hyperviseur

- Shadow page tables : l'OS a son propre ensemble de pages distinct de celui du niveau physique
  - L'hyperviseur valide les modifications faites par l'OS et les transfère au niveau physique
- En pratique, l'OS a un accès direct en lecture seulement aux pages du niveau physique, et l'hyperviseur contrôle l'écriture uniquement

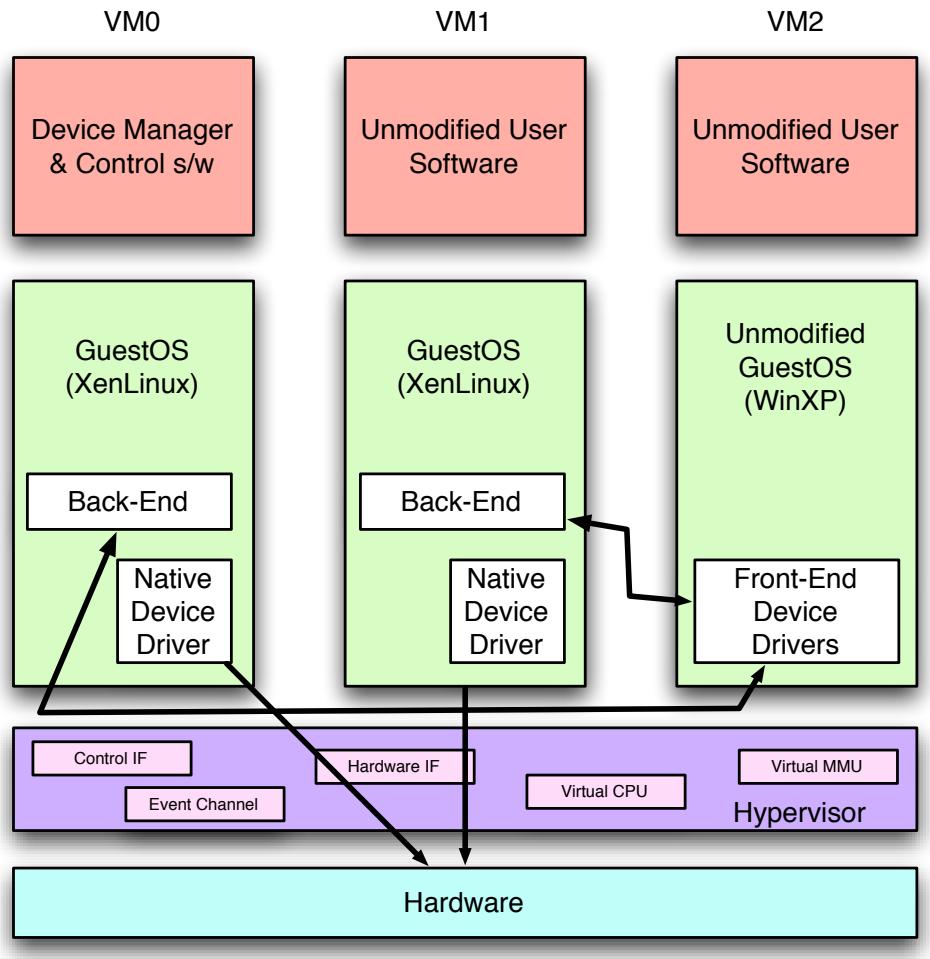
Description de XEN : I/O

- Au démarrage, Xen démarre dom0, le premier domaine privilégié
- dom0 a accès à toute la couche physique du système
- dom0 exporte un sous-ensemble des périphériques matériel du systèmes aux autres domaines
- les périphériques sont exportés via des device channels

Description de XEN : I/O (suite)

- dom0 exécute le backend de chaque matériel, qui est exporté pour chaque domaine via un frontend
  - netback, netfront
  - blockback, blockfront
  - PCI pass through
- Les autres domaines peuvent se voir accorder un accès physique à un périphérique (attention sécurité)
- Configuration PCI virtuelle, interruptions virtuelles

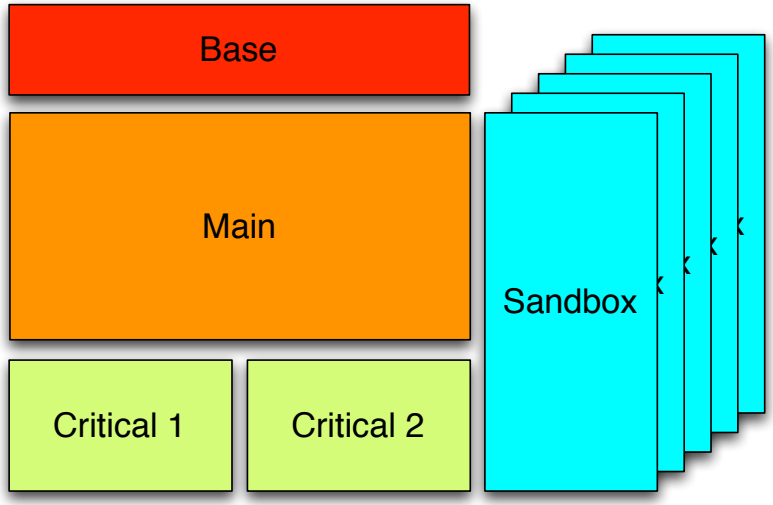
Description de XEN : architecture



Vulnérabilité de Xen selon le CERTA

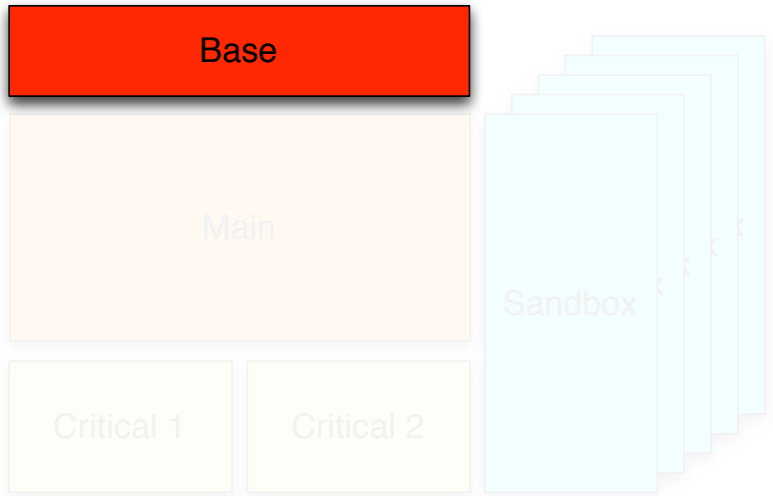
- CERTA-2008-AVI-429
  - Risques : Exécution de code arbitraire en local, contournement de la politique de sécurité.
  - Gestion des appels flask_op
- CERTA-2007-AVI-532
  - Risque : Contournement de la politique de sécurité.
  - Xen 3.1.2, architecture IA64
- CERTA-2007-AVI-197
  - Accélération physique dans XEN = accélération physique dans QEMU $\Longrightarrow$ mêmes risques potentiels
  - Risques (QEMU) : Exécution de code arbitraire, déni de service, contournement de la politique de sécurité.
  - QEMU 0.x, non prouvé sur XEN

SAFE-OS : Architecture



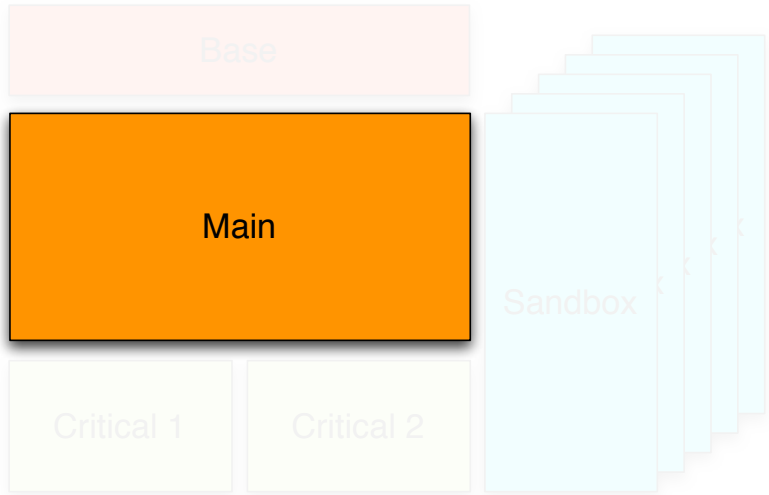
- Le système SAFE-OS est constitué d'un nombre variable de machines virtuelles
- Chaque machine virtuelle possède son propre niveau de sécurité, et ses applications dédiées
- Les machines virtuelles sont toutes instanciées au démarrage de la machine physique

SAFE-OS : Architecture



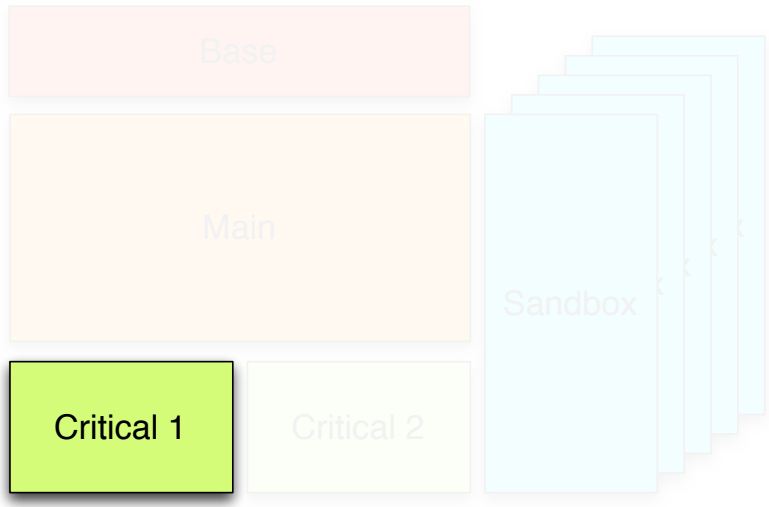
- Le système de base (Dom0) n'exécute aucun service réseaux, aucune application utilisateur non plus (à l'exception du login et de l'agent ssh)
- Il héberge les services de base du réseau virtuel (DNS, routage)
- Il est responsable de la politique de blocage des communications entre les différentes machines virtuelles
- Il héberge les clés privées de l'utilisateur qui sont exportées

SAFE-OS : Architecture



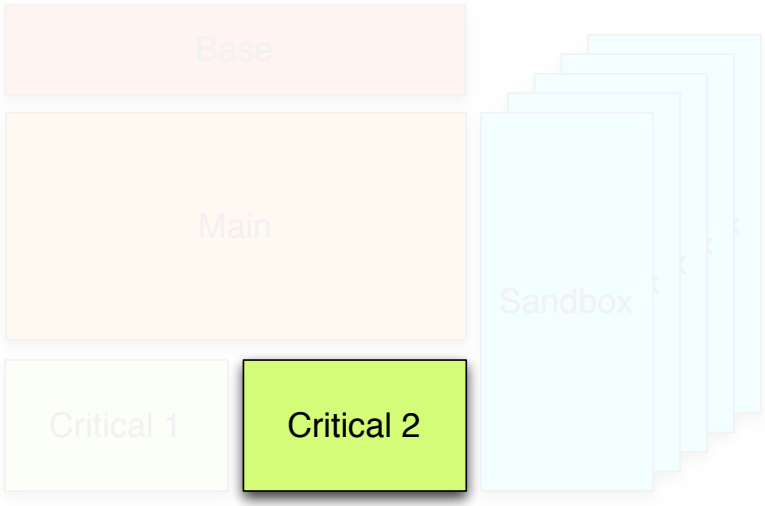
- Le système main (Dom1) n'exécute pas de service connecté à l'extérieur (politique de firewall contraignante)
- Il héberge les données générales de l'utilisateur
- C'est dans le système de base que s'exécute le gestionnaire de fenêtres de l'utilisateur

SAFE-OS: Architecture



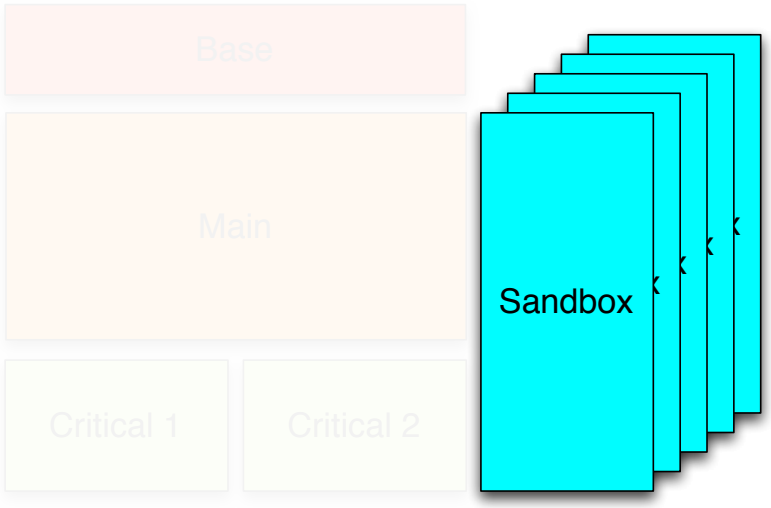
- Le système critique 1 héberge le browser web pour la navigation sur les sites critiques (impôts, etc.)
- Il héberge les données relatives à ces sites critiques
- On assume que les pages présentées par ces sites critiques (s'ils sont correctement authentifiés) sont saines

SAFE-OS : Architecture



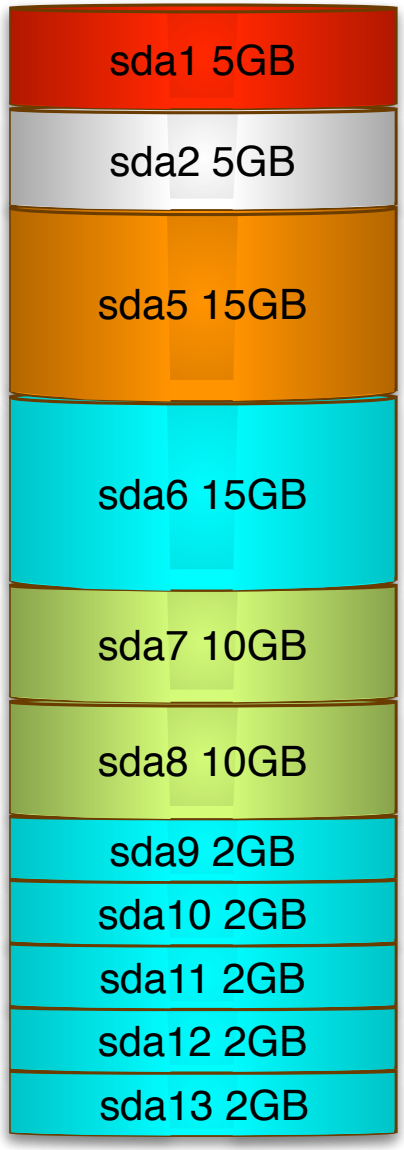
- Le système critique 2 héberge le client mail de l'utilisateur
- Même si le serveur est authentifié
- Il héberge les données relatives au client mail
- A la différence des sites critiques, même si le serveur de mail est correctement authentifié, les mails qu'il renvoie peuvent être corrompus et/ou transporter des virus.

SAFE-OS : Architecture



- Les bacs à sable hébergent les applications connectées à l'extérieur, potentiellement sur des sites non certifiés
- Ces applications ne doivent pas être utilisées pour contacter les sites critiques
- Chaque instance est réinitialisable à la demande pour supprimer les données corrompues

SAFE-OS : Partitionnement typique



Boot - Base system

Swap

LVM MainEnv

LVM SandBox (ro)

LVM Critical1

LVM Critical2

LVM SB0 (cow)

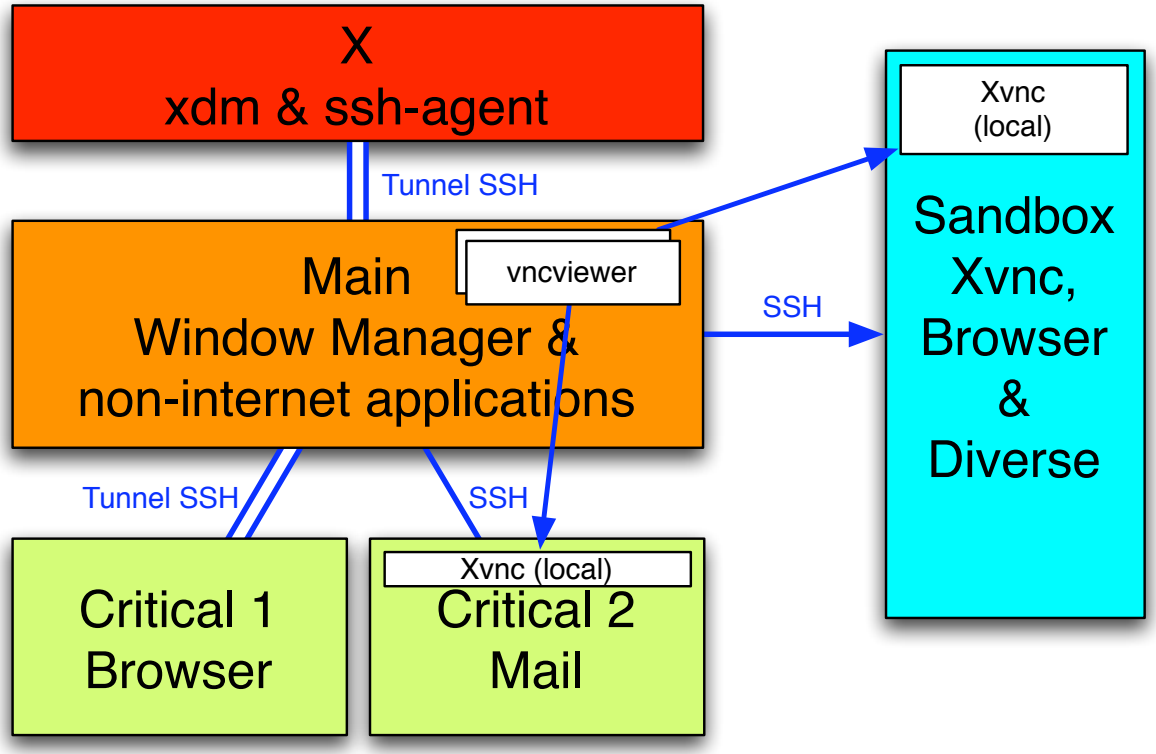
LVM SB1 (cow)

LVM SB2 (cow)

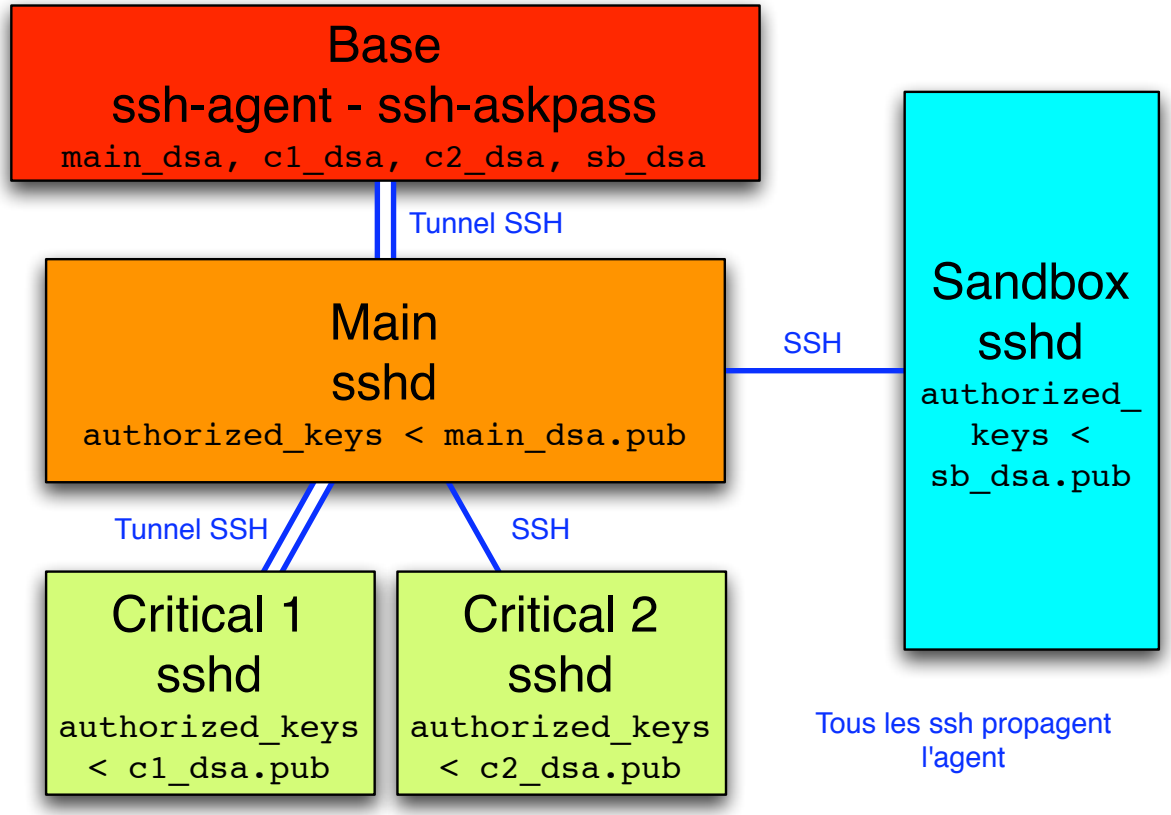
LVM SB3 (cow)

LVM SB4 (cow)

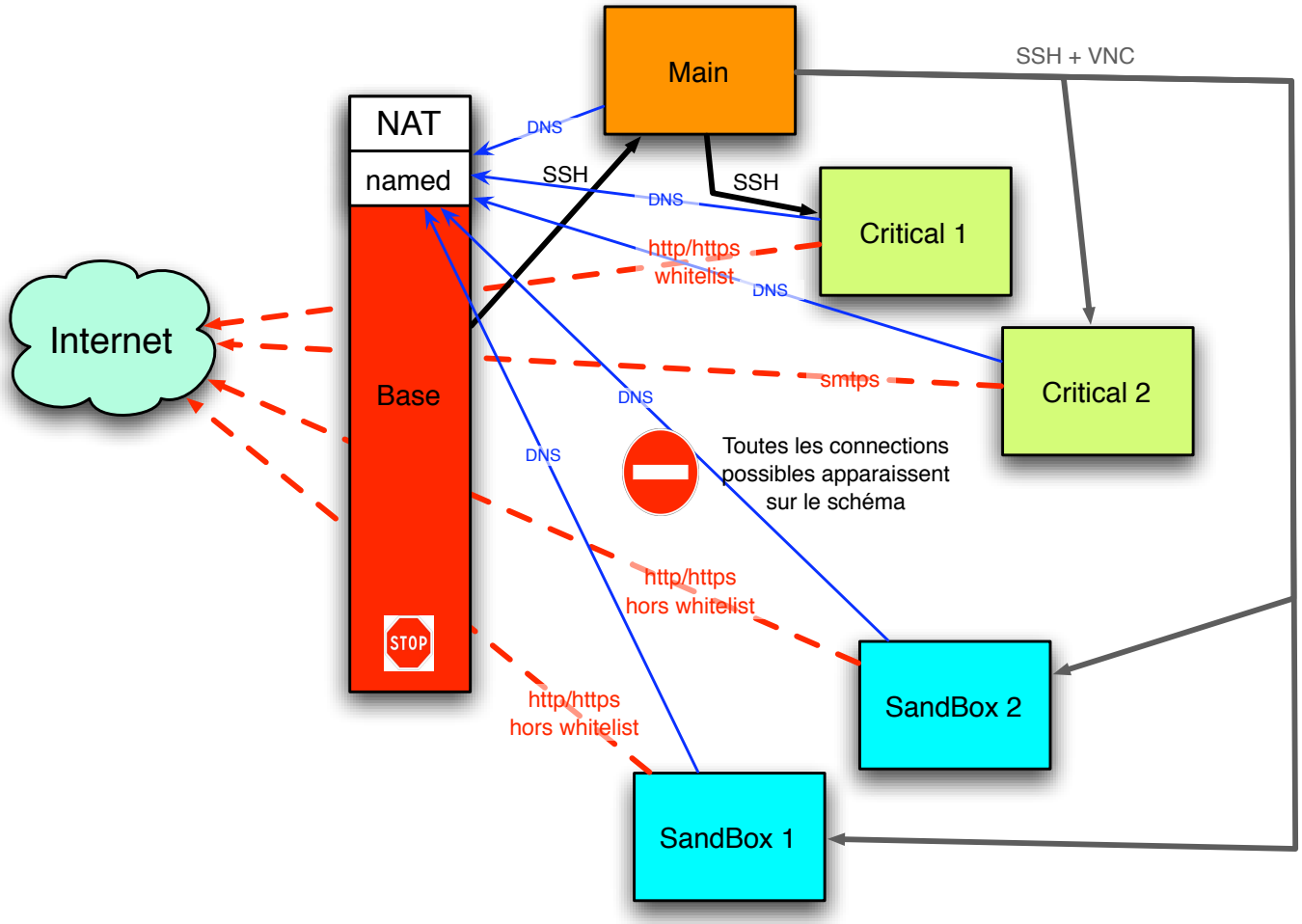
SAFE-OS : Affichage - X



SAFE-OS : ssh entre machines virtuelles



SAFE-OS : Firewalls

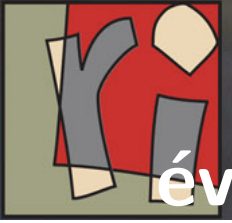


Gestion du projet : état des lieux

- Prototype fonctionnel conçu par les permanents du projet
- Packaging (distribution) non aboutie
- Fonctionalités non terminées (voir évolutions)
- Problèmes de recrutement sur la première période de développement
  - Spécialiste des machines virtuelles sur poste au LIP6
  - Multiples négociations qui ont échoué sur un CDD de deux ans avec de multiples candidats (Aida Saydane, Nicolas Néri, Jean-Philippe Garcia-Ballester, Hugo Jardonnet, Viven Delmon, Florient Lesaint, Jimmy Ma, ...)
  - Les grilles de salaires de l'université sont un frein au recrutement dans l'état actuel du marché
  - Plusieurs propositions de stage, une a aboutie. Début en avril (Mehdi Kennani)

Gestion du projet : recrutements en cours

- postdoc / ingénieur en CDD : Ala Rezmerita (début en septembre 2009)
- transformation du stage de Mehdi Kennani en CDD de un an en septembre 2009.



Gestion du projet : prochaine phase - évaluation

Nous avons constitué une équipe pour la première phase d'évaluation :

- Thomas Largillier (Doctorant, Université Paris-Sud, en thèse dans l'équipe)
- Alexandre Borghi (Doctorant, Université Paris-Sud, en thèse dans l'équipe)
- Mehdi Kennani (Stagiaire de Master Recherche, Université Paris 6, début avril 2009)
- Sébastien Tixeuil (Pr., Université Paris 6, permanent)
- Thomas Hérault (MdC, Université Paris-Sud, permanent)
- Sylvain Peyronnet (MdC, Université Paris-Sud, permanent)

SAFE-OS : Distribution / Déploiement

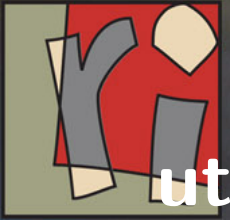
- Distribution non encore “packagée”
- Distribuable en l’état : images virtuelles, image de base
- Plusieurs solutions sont envisagées pour la phase d’évaluation :
  1. fournir un dvd avec les images virtuelles, et une copie de l’image de base du prototype fonctionnel.
  2. fournir un how-to pour créer l’installation à partir d’une debian lenny basique.
  3. installer le système sur les machines d’évaluation achetés pour SAFE-OS, et prêter ces machines aux autres équipes, avec disque de récupération

Évolutions prévues : déploiement

- La première tâche de la phase de développement consistera à empaqueter la solution proposée pour permettre l'installation comme un système d'exploitation "normal"
- Debian customisée
- Cette tâche est commencée, elle continuera lors de la première phase d'évaluation, en parallèle de l'évaluation
- La première version installable "normalement" sera disponible avant le 1er Juillet 2009.

Évolutions prévues : mises à jour

- Le prototype fonctionnel actuel utilise les mises à jour authentifiées fournies par debian (`apt-get update`; `apt-get upgrade`).
- ces mises à jour doivent être effectuées par le super-utilisateur, sur chacune des machines virtuelles
- la mise à jour de Xen lui-même peut poser des problèmes.
- La seconde tâche de la phase de développement va consister à fournir une automatisation de ces mises à jour sur les différentes machines virtuelles



Évolutions prévues : gestion des utilisateurs et de leurs clés

- Dans le prototype actuel, les utilisateurs doivent exister sur chaque machine virtuelle, avec le même identifiant.
- La création et la distribution des clés est une tâche du super-utilisateur.
- La gestion des utilisateurs, de leurs clés et de la distribution de ces clés sur les machines virtuelles devra être automatisée.

Evolutions prévues : migrations de fichiers entre VM

- Les migrations de fichiers entre machines virtuelles sont possible aujourd'hui, via ssh / scp / sftp
- Ces opérations ne sont pas transparentes pour l'utilisateur, qui doit connaître l'architecture globale, et la localisation des fichiers sur le système distribué
- Des outils pour permettre à l'utilisateur de déplacer les données seront développés

Evolutions prévues : XSM

- Xen fournit un module de sécurité (Xen Security Module), qui permet de contrôler au niveau du Dom0 les appels à l'hyperviseur par les autres domaines
- Ce module permet de vérifier à un niveau plus bas que les entrées/sorties réseaux le comportement des machines virtuelles
- Ce module a malheureusement introduit des failles de sécurité (CERTA-2008-AVI-429). Son utilisation est en cours d'évaluation

Questions ?


42% 56% 2% 0%
A • B • C • D
Qu'est-ce qui gravite autour de la Terre ?
A: La Lune
B: Le Soleil
C: Mars
D: Vénus