Retour d'expérience en grande entreprise : Sécurité & logiciels libres, des projets novateurs et rentables

Convention Sécurité 2005

16 juin 2005, Paris

Bruno KEROUANTON
Responsable Sécurité & Nouvelles Technologies
Clear Channel France

I – Présentation du périmètre

Clear Channel, c'est :

… dans le monde :

- Le leader mondial de la communication extérieure.
- Groupe américain (San Antonio, Texas).
- Activités dans 65 pays.
- 1400 stations de radio, 37 chaînes de télévision, organisation de spectacles et d'évènements, affichage extérieur, mobilier urbain.

… en France :

- 1850 collaborateurs, 31 agences et 17 bureaux.
- Spécialiste en affichage extérieur : mobilier urbain, bus et métros, gares et trains, centres commerciaux, parkings.

I – Passerelle de messagerie internet

CONTEXTE

- 1850 utilisateurs référencés,
- 12000 adresses e-mail pour le personnel en interne.

- Serveur de messagerie interne sous MS Exchange, et le métamoteur anti-virus Sybari Antigen (sans anti-spams).

- Passerelle de messagerie Windows, avec anti-virus « vieillissant », et ne traitant pas les spams.

CONSTAT PESSIMISTE

- De plus en plus de spams envahissent les boîtes aux lettres.
- Les virus de l'été 2003 ont laissé s'échapper de nombreuses adresses à usage interne.
- Le serveur Exchange commence à saturer.

SOLUTION

- Mise en place d'une nouvelle passerelle de messagerie Internet.

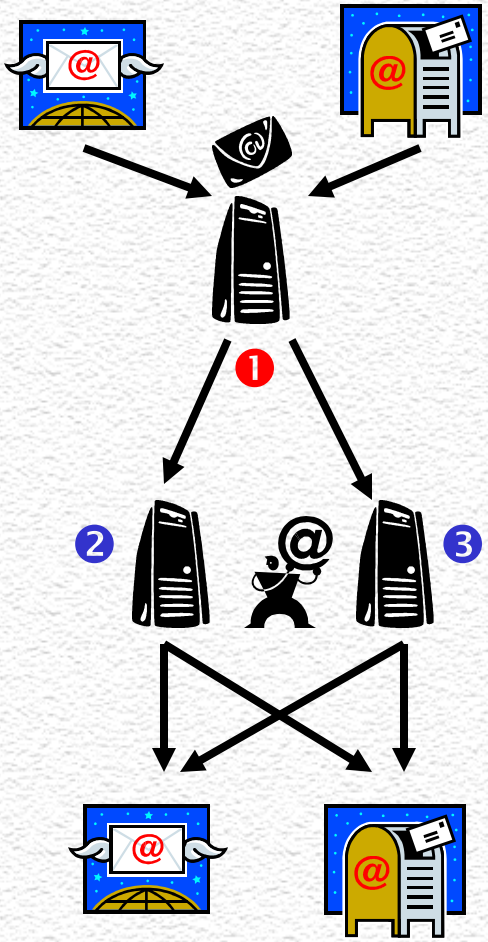
- Contraintes imposées :

  – Redimensionnable facilement en fonction des flux et besoins.
    - Utilisation de plusieurs serveurs, avec répartition de charge.

  – Pas/peu de maintenance, autonomie du système.
    - L'équipe informatique n'intervient pas
    - Le système apprend « tout seul », et les utilisateurs peuvent interagir.

  – Coût faible.

ASPECTS MATERIELS



- Trois serveurs identiques matériellement.
  - Environnement virtualisé (Vmware ESX)
  - 128Mo de mémoire, 4Go de disque dur.
- Un serveur de messagerie « frontal » ❶
  - Fonction de réception et de préqualification des messages
- Deux serveurs identiques de traitement ❷,❸
  - Gestion des virus et des spams
  - Transmission des messages en interne et en externe

ASPECTS LOGICIELS

- Linux Debian 3.0 (Woody)
- Logiciel de messsagerie (MTA) : EXIM v3
- Traitement des SPAMs : Spam-Assassin
- Traitement anti-virus : Clam-AV
- Intégration de la solution : Amavis-ng, scripts Perl
- Interfaçage Active Directory : scripts Perl et OpenLDAP

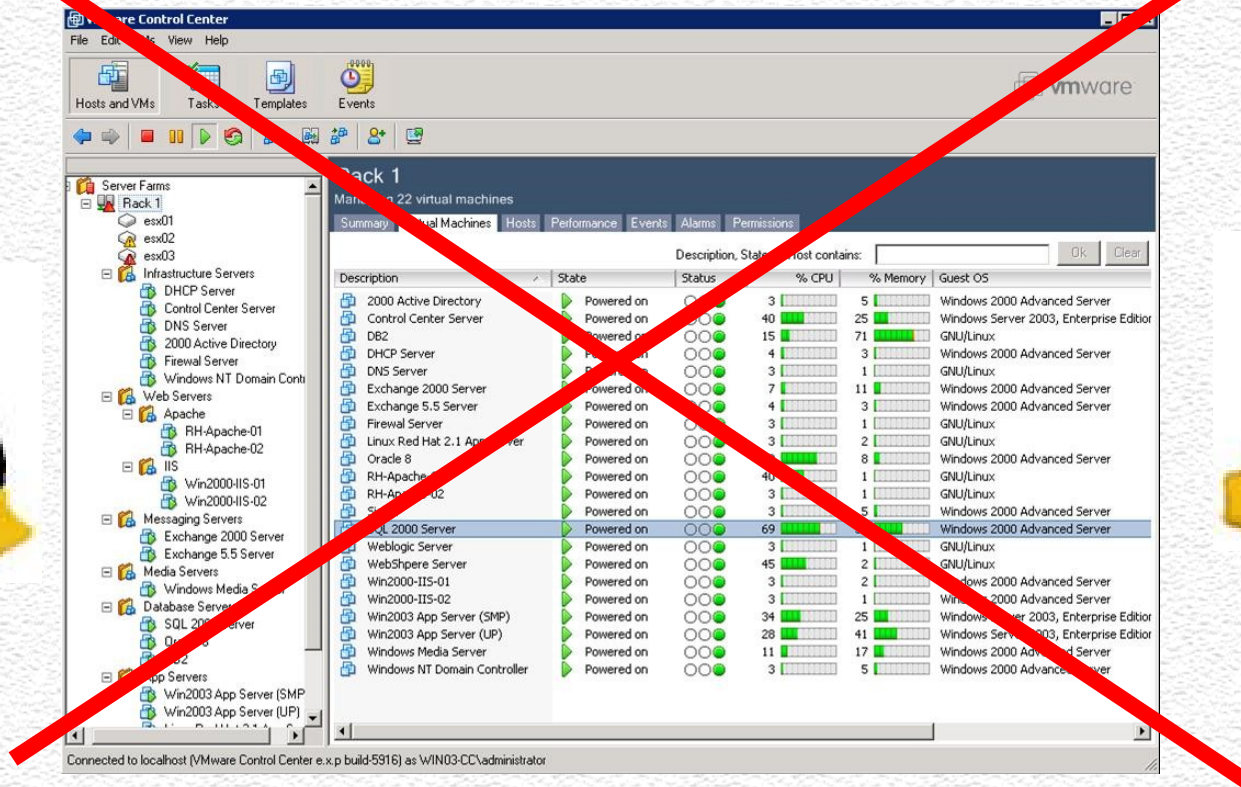
AVANTAGES

- Auto-apprentissage de l'anti-SPAMs
  - Filtres Bayésiens auto-alimentés périodiquement
  - Traitement automatique des messages mal étiquetés, transférés par les utilisateurs .
  - ➔ Pas de maintenance !
- Suppression de 98% des messages nuisibles en entrée
  - Vérification de la structure du message (en-tête etc…)
  - Intégration avec Active Directory : vérification des utilisateurs
  - ➔ Soulage le serveur interne de messagerie
- Pas de maintenance
  - Mise à jour automatique et périodique des correctifs de sécurité et signatures de virus.
  - Fonctionne en « boîte noire » (auto-nettoyage des fichiers journaux etc.)
  - ➔ Frais d'exploitation réduits

RESSOURCES :

- Linux Debian :
  http://www.debian.org
- Anti-virus libre Clam-AV :
  http://www.clamav.net
- Amavis :
  http://www.amavis.org
- Logiciel de messagerie EXIM :
  http://www.exim.org
- Anti-Spams SpamAssassin :
  http://spamassassin.apache.org

II – Réplication à chaud de l'infocentre

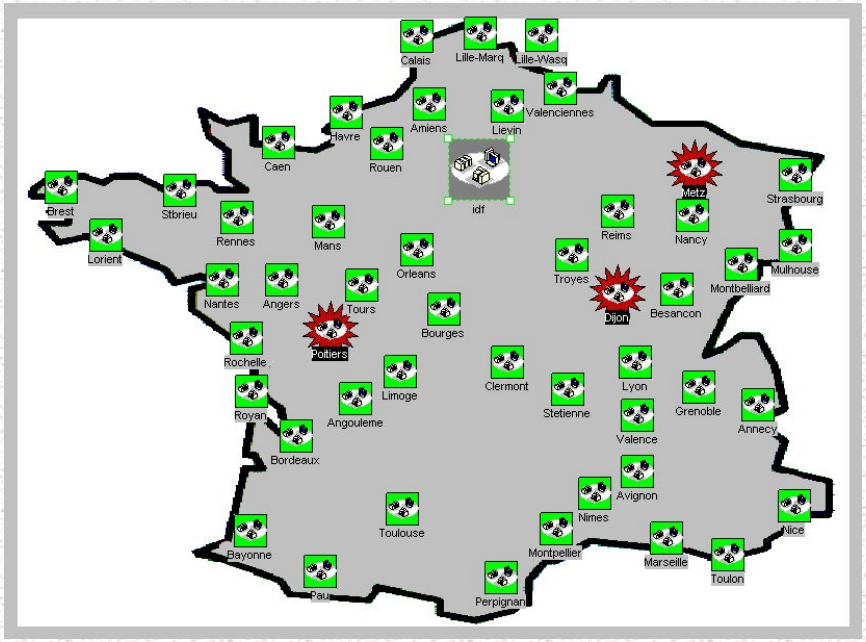


Désolé !

III – Supervision nationale des flux réseaux

CONTEXTE :

- 31 agences, 17 bureaux, répartis sur tout le territoire.
- De 1 à 160 utilisateurs sur les sites de province.



- Différents moyens de communication utilisés, dont : xDSL, LS.
- Flux transitant entre Paris (Siège) et les agences.

III – Supervision nationale des flux réseaux

CONSTAT PESSIMISTE :

- Aucune visibilité réelle concernant les types de flux d'agences :
  - Prospective difficile pour la gestion de l'infrastructure réseau.
- Pas de maîtrise de la bande passante :
  - Lenteurs aléatoires sur certains applicatifs métier.
- Pas de filtrage des applications interdites en interne :
  - Logiciels de peer-to-peer, messagerie instantanée, etc.

III – Supervision nationale des flux réseaux

OBJECTIFS :

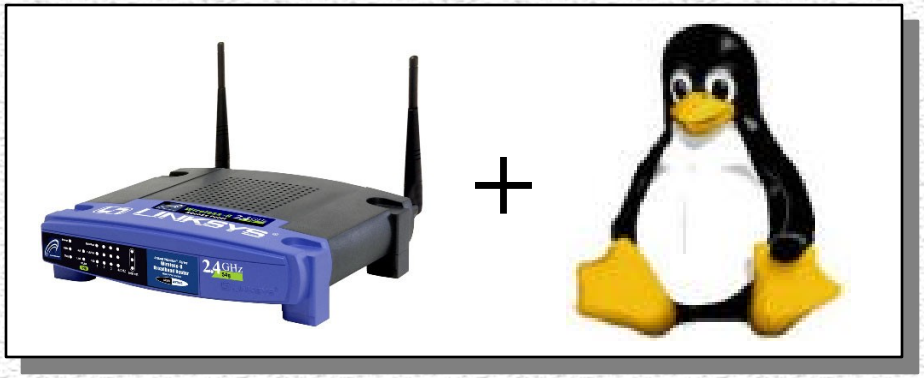
- Mettre en place des équipements dans chaque agence.
- Remonter les statistiques de trafic au siège.
- Transparent pour les utilisateurs.
- Dépenser le moins possible !
- Projet démarrant normalement au 2ème semestre 2005

PARTIE MATERIELLE :

- Utilisation de routeurs « grand public » Linksys (Cisco).
- Moins de 100 Euros pièce !
- 48 sites ➔ 4800 Euros…
- Suppression des antennes (et désactivation du Wi-Fi par logiciel)

PARTIE MATERIELLE (2) :

- Processeur MIPS à 125 MHz
- 16 Mo de RAM



C’est un VRAI serveur Linux !

PARTIE MATERIELLE (3) :

- Chipset ADM6996L
  - 6 port 10/100 Mbit/s Single chip Ethernet Switch Controller
  - 802.1p (QoS) : Gestion de la bande passante
  - 802.1q (VLAN)
  - Bloquage des ports par Mac-Adresse
  - Gestion avancée des ports
  - Auto MDI-x
  - Gestion des priorité par port, VLAN, et champ IP TOS.
  - Assignation jusqu'à 16 groupes de VLANs

C'est un VRAI switch manageable !

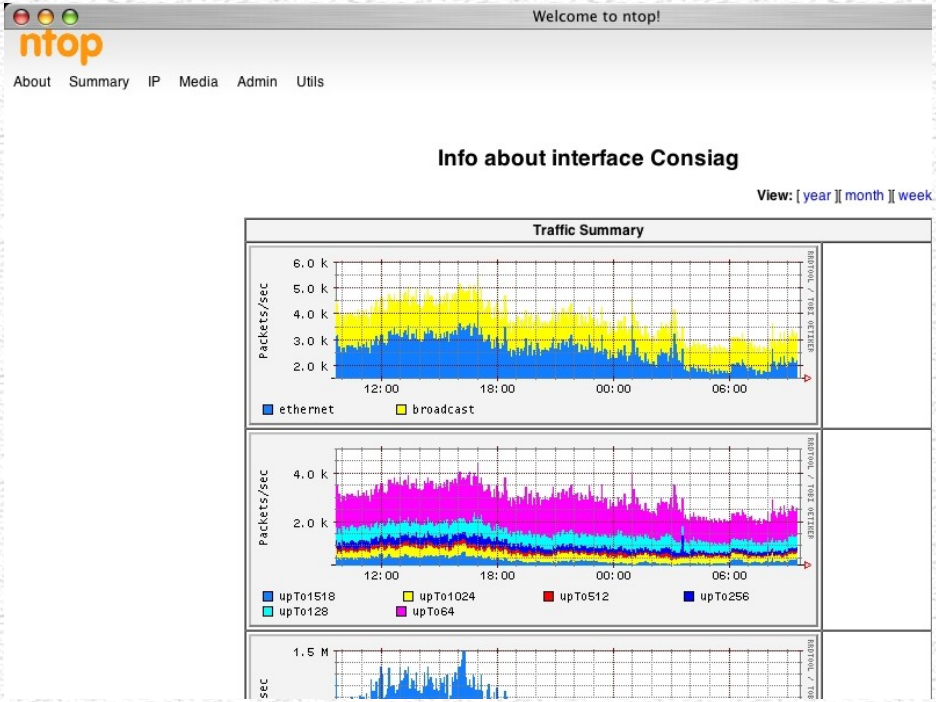
PARTIE LOGICIELLE :

- Microcode personnalisé par SVEASOFT pour le routeur WRT-54G
  - Noyau LINUX 2.4
  - Fonctions réseaux avancées :
    - QoS complet
    - Firewall applicatif (niveau 2 à 7)
    - Filtrage des flux par mots clefs, IP, application, mac-adresse, etc…
  - Pilotage complet du chipset ADM9669
- Coût du microcode + support : 20 $ par an !

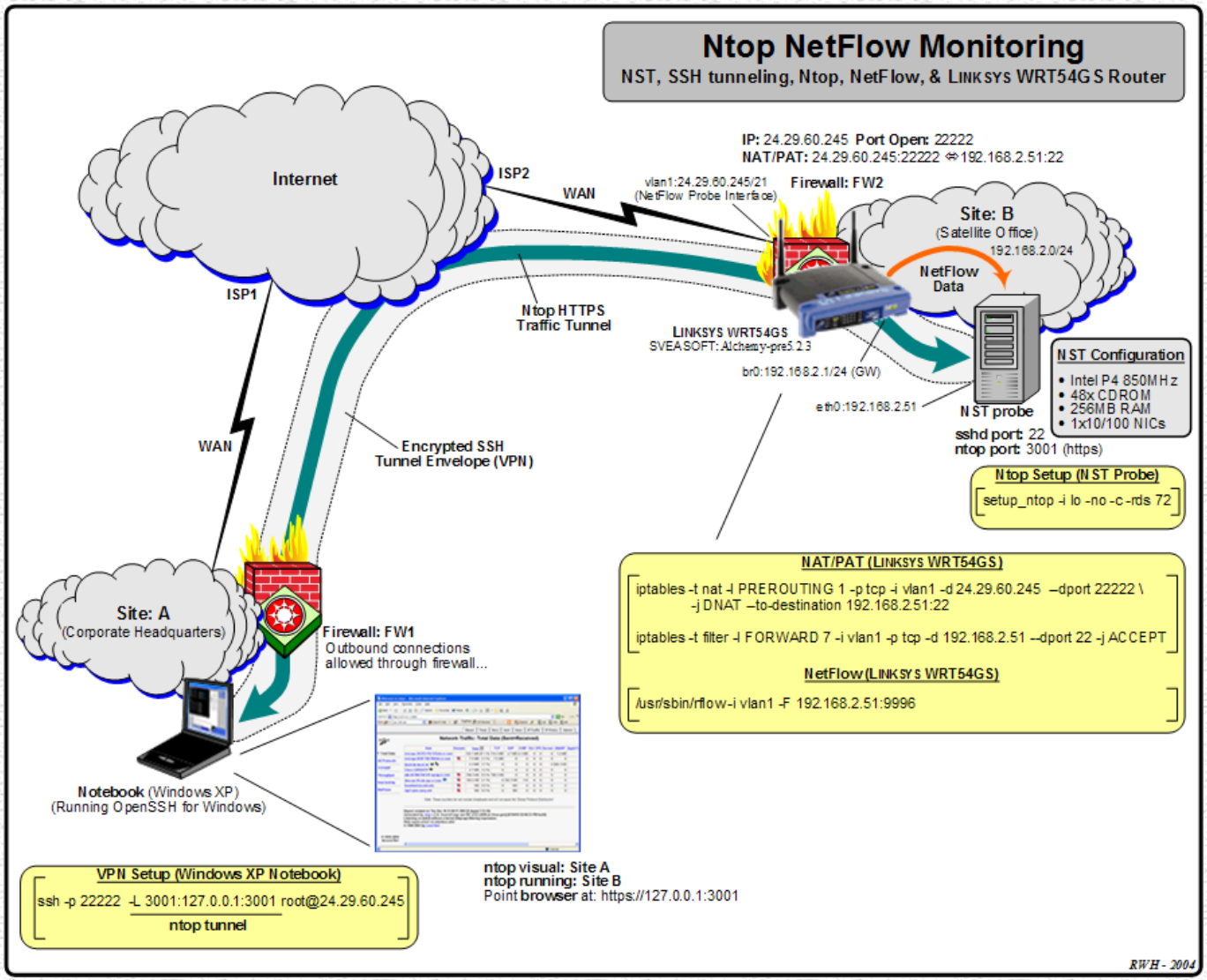
III – Supervision nationale des flux réseaux

SITE CENTRAL :

- Serveur de collecte sous Linux Debian
- Récupération des flux statistiques NetFlow / Rmon
- Intégration avec le logiciel libre NTOP



III – Supervision nationale des flux réseaux



RESSOURCES :

- Site officiel Linksys :
  http://www.linksys.com
- Site officiel microcode Sveasoft :
  http://www.sveasoft.com
- « Ntop NetFlow with a WRT54GS Firewall/Router and NST Probe » :
  http://nst.sourceforge.net/nst/docs/user/ch09s02.html

Questions ?