

Session N° 22 – Logiciels libres et sécurité

DEUX PROJETS NOVATEURS ET RENTABLES

Bruno Kerouanton – CISSP
Responsable Sécurité & Nouvelles Technologies
CLEAR CHANNEL France

bruno@kerouanton.net

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 :

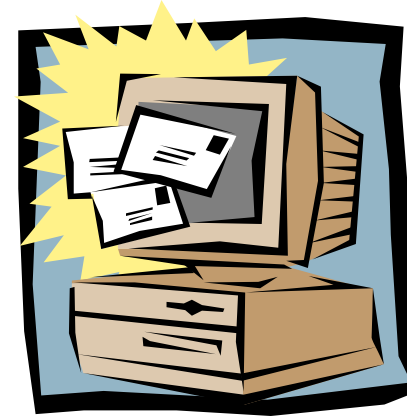
- ❑ 1850 collaborateurs, 31 agences et 17 bureaux.
- ❑ Spécialiste en affichage extérieur : mobilier urbain, bus et métros, gares et trains, centres commerciaux, parkings.



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.



I – Passerelle de messagerie Internet

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.



I – Passerelle de messagerie Internet

SOLUTION

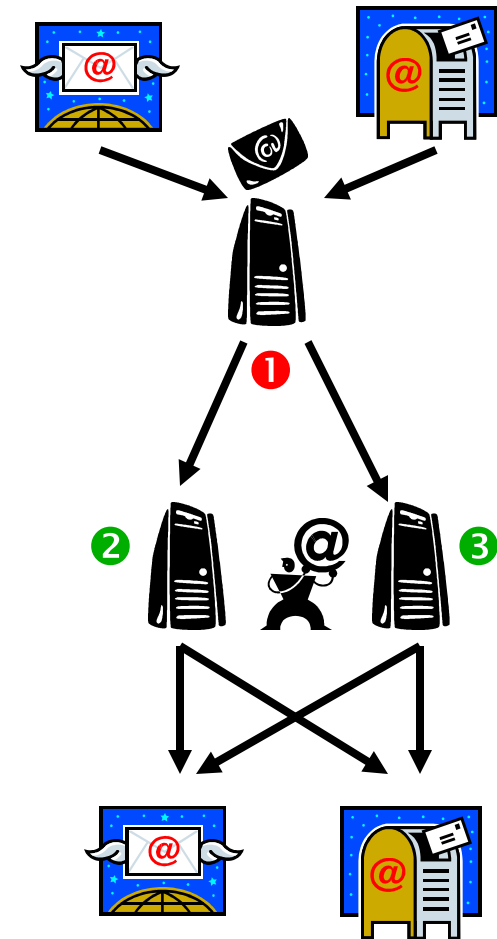
- **Mise en place d'une nouvelle passerelle de messagerie Internet.**
- **Contraintes imposées :**
 - **Redimensionnable facilement en fonction des flux et besoins.**
 - Utilisation de plusieurs serveurs, avec répartition de charge.
 - **Pas/peu de maintenance, autonomie du système.**
 - L'équipe informatique n'intervient pas
 - Le système apprend « tout seul », et les utilisateurs peuvent interagir.
 - **Coût faible.**



I – Passerelle de messagerie Internet

ASPECTS MATERIELS

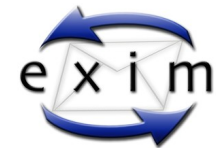
- **Trois serveurs identiques matériellement.**
 - Environnement virtualisé (Vmware ESX)
 - 128Mo de mémoire, 4Go de disque dur.
- **Un serveur de messagerie « frontal » ①**
 - Fonction de réception et de préqualification des messages
- **Deux serveurs identiques de traitement ②,③**
 - Gestion des virus et des spams
 - Transmission des messages en interne et en externe



I – Passerelle de messagerie Internet

ASPECTS LOGICIELS

- Linux Debian 3.0 (Woody)
- Logiciel de messagerie (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



I – Passerelle de messagerie Internet

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

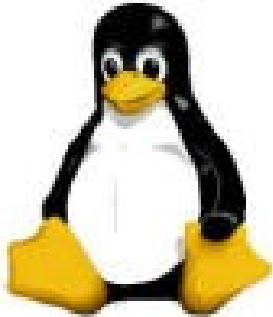
I – Passerelle de messagerie Internet

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



Description	Status	Power	% CPU	% Memory	Guest OS
2000 Active Directory	Powered on	●●●○	3	5	Windows 2000 Advanced Server
Control Center Server	Powered on	●●●○	40	25	Windows Server 2003, Enterprise Edition
DB2	Powered on	●●●○	15	71	GNU/Linux
2000 Active Directory	Powered on	●●●○	4	3	Windows 2000 Advanced Server
DHCP Server	Powered on	●●●○	3	1	GNU/Linux
DNS Server	Powered on	●●●○	7	11	Windows 2000 Advanced Server
Exchange 2000 Server	Powered on	●●●○	3	3	Windows 2000 Advanced Server
Exchange 5.5 Server	Powered on	●●●○	3	1	GNU/Linux
Firewal Server	Powered on	●●●○	3	1	GNU/Linux
Linux Red Hat 2.6 App Server	Powered on	●●●○	3	2	GNU/Linux
Oracle 8	Powered on	●●●○	63	1	Windows 2000 Advanced Server
RH-App-01	Powered on	●●●○	40	1	GNU/Linux
RH-App-02	Powered on	●●●○	3	1	GNU/Linux
Web Server	Powered on	●●●○	3	5	Windows 2000 Advanced Server
SQL 2000 Server	Powered on	●●●○	69	50	Windows 2000 Advanced Server
Weblogic Server	Powered on	●●●○	3	1	GNU/Linux
WebSphere Server	Powered on	●●●○	45	2	GNU/Linux
Win2000-IIS-01	Powered on	●●●○	3	2	Windows 2000 Advanced Server
Win2000-IIS-02	Powered on	●●●○	3	1	Windows 2000 Advanced Server
Win2003 App Server (SMP)	Powered on	●●●○	34	25	Windows Server 2003, Enterprise Edition
Win2003 App Server (UP)	Powered on	●●●○	28	41	Windows Server 2003, Enterprise Edition
Win2003 App Server	Powered on	●●●○	11	17	Windows 2000 Advanced Server
Windows NT Domain Controller	Powered on	●●●○	3	5	Windows 2000 Advanced Server

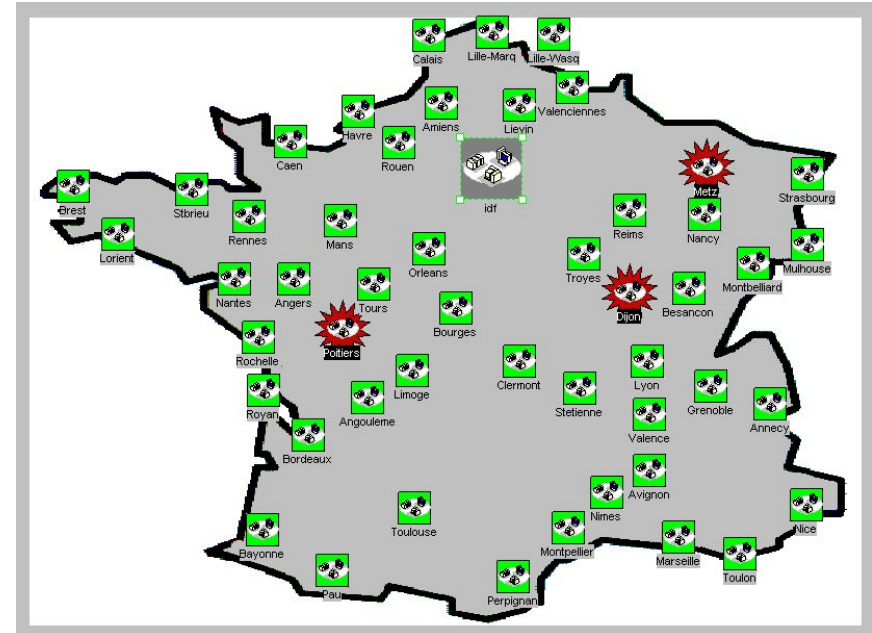


Désolé !

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

III – Supervision nationale des flux réseaux

PARTIE MATERIELLE :

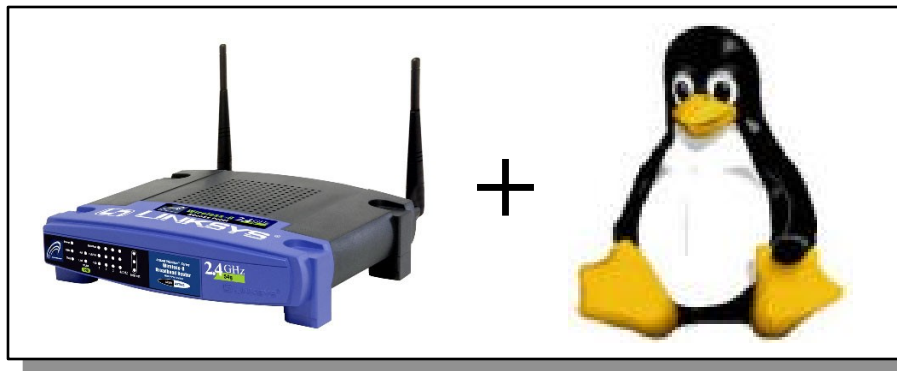
- Utilisation de routeurs « grand public » Linksys (Cisco)
- Moins de 100 Euros pièce !
- 48 sites → 4800 Euros...
- Suppression des antennes (et désactivation du Wi-Fi par logiciel)



III – Supervision nationale des flux réseaux

PARTIE MATERIELLE (2) :

- Processeur MIPS à 125 MHz
- 16 Mo de RAM



C'est un VRAI serveur Linux !

III – Supervision nationale des flux réseaux

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 !

III – Supervision nationale des flux réseaux

PARTIE LOGICIELLE :

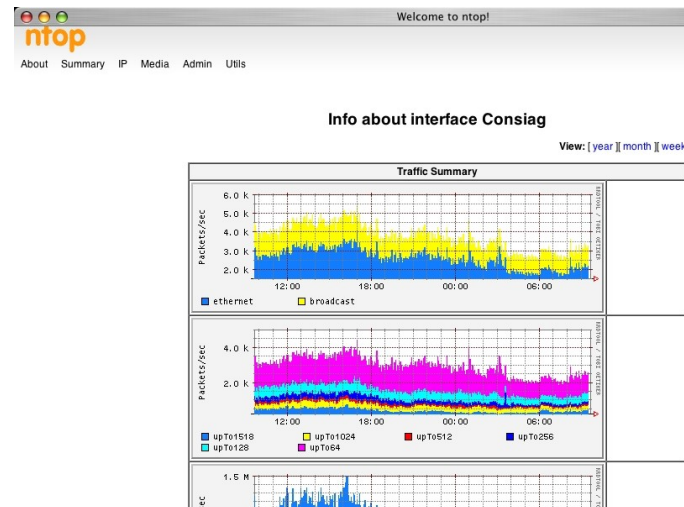
- **Microcode personnalisé par SVEASOFT pour le routeur WRT-54G**
 - **Noyau LINUX 2.4**
 - **Fonctions réseaux avancées :**
 - **QoS complet**
 - **Firewall applicatif (niveau 2 à 7)**
 - **Filtrage des flux par mots clefs, IP, application, mac-adresse, etc...**
 - **Pilotage complet du chipset ADM9669**

- **Coût du microcode + support : 20 \$ par an !**

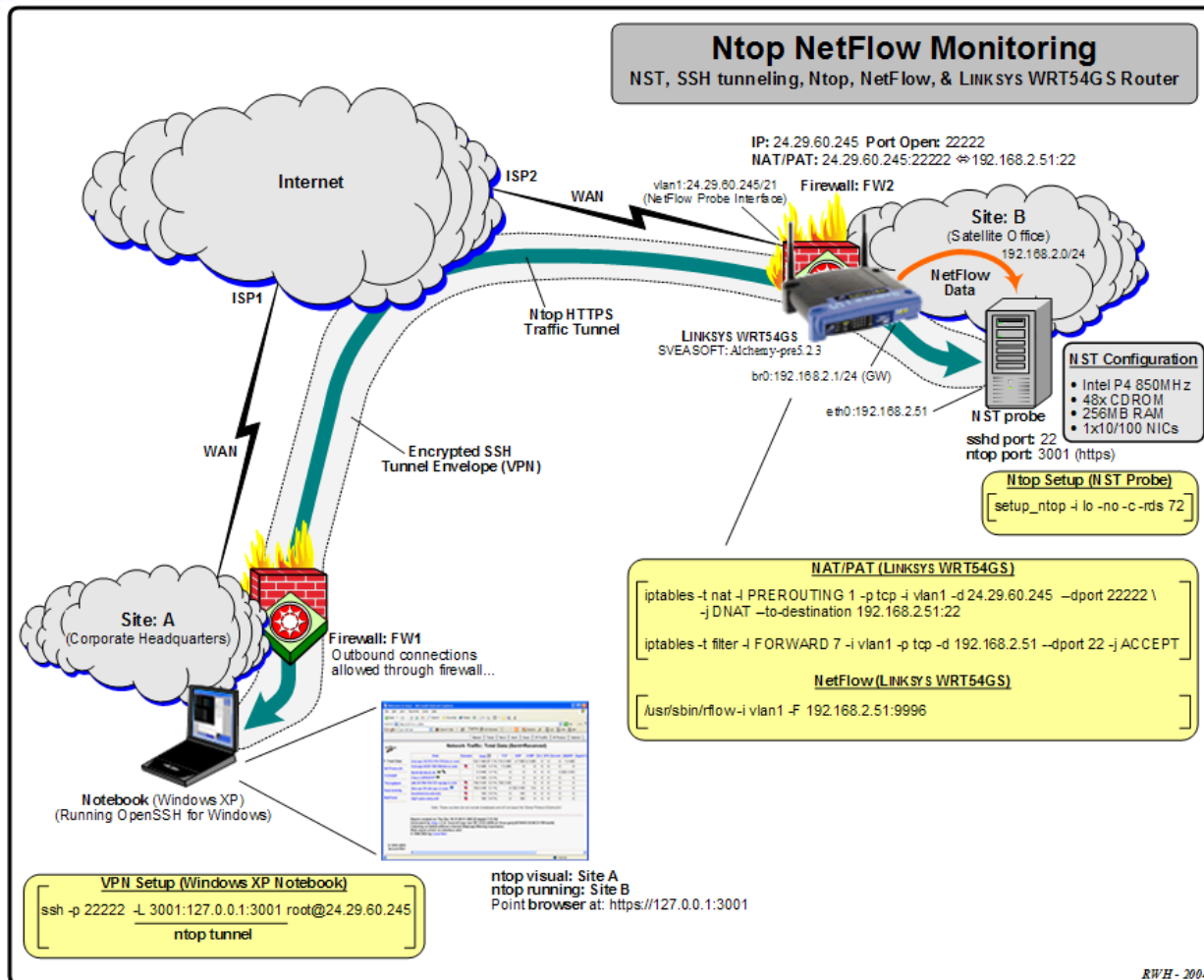
III – Supervision nationale des flux réseaux

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



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 ?

