Infrastructures de gestion des journaux informatiques

Frédéric Sauveur

Coordination SSI Université de Grenoble

D’après les recommandations de l’ANSSI

Pourquoi des journaux ?

- Diagnostiquer un problème
- Être alerté d'un dysfonctionnement
- Surveiller le bon fonctionnement
- Garder des traces de l'activité
- Facturer le service
- Faire des statistiques
- Respecter la règlementation
- Dissuader d'agir contre les règles

Préalable

- L’application est capable de journaliser
- Disposer d’une base de temps fiable
- Choisir les informations à journaliser
- Définir la durée de conservation et la politique d’archivage
- S’engager à consulter régulièrement les journaux

Horodatage

Synchronisation régulière de toutes les horloges

- NTP, GPS, radio. Attention aux fuseaux horaires
- Chaque évènement est horodaté individuellement
- Indispensable pour l'analyse après incident

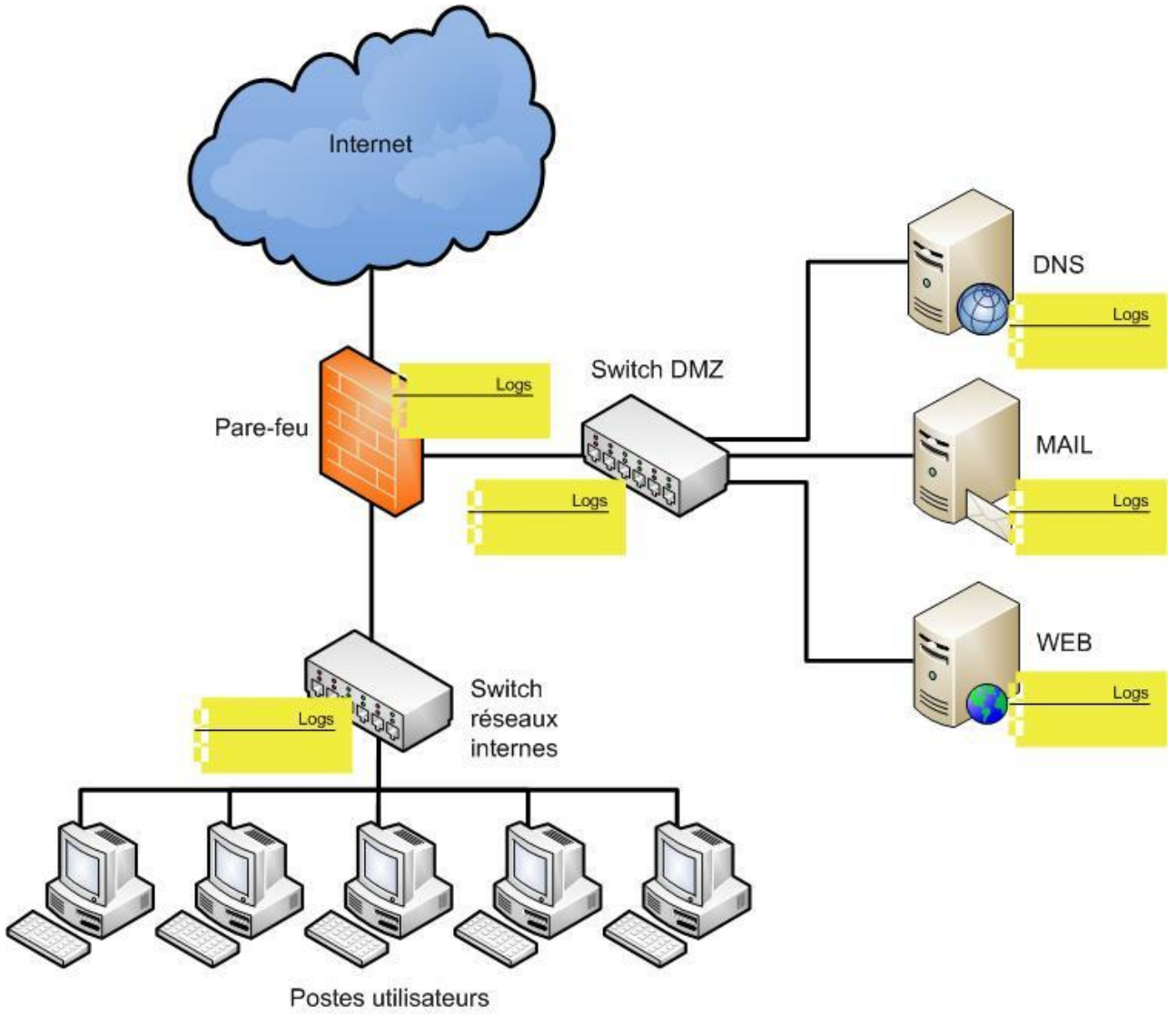
Intégrité

Eviter l'effacement des journaux sur une machine

Hacker, défaillance

- Déporter les journaux sur une autre machine en temps réel, les centraliser (ex : syslog-ng sous Linux, snare sous Windows)
- Les archiver sur un autre media, en étant vigilant sur les capacités de stockage et sur les durées de conservation (2e serveur syslog, sauvegardes, DVD, …)

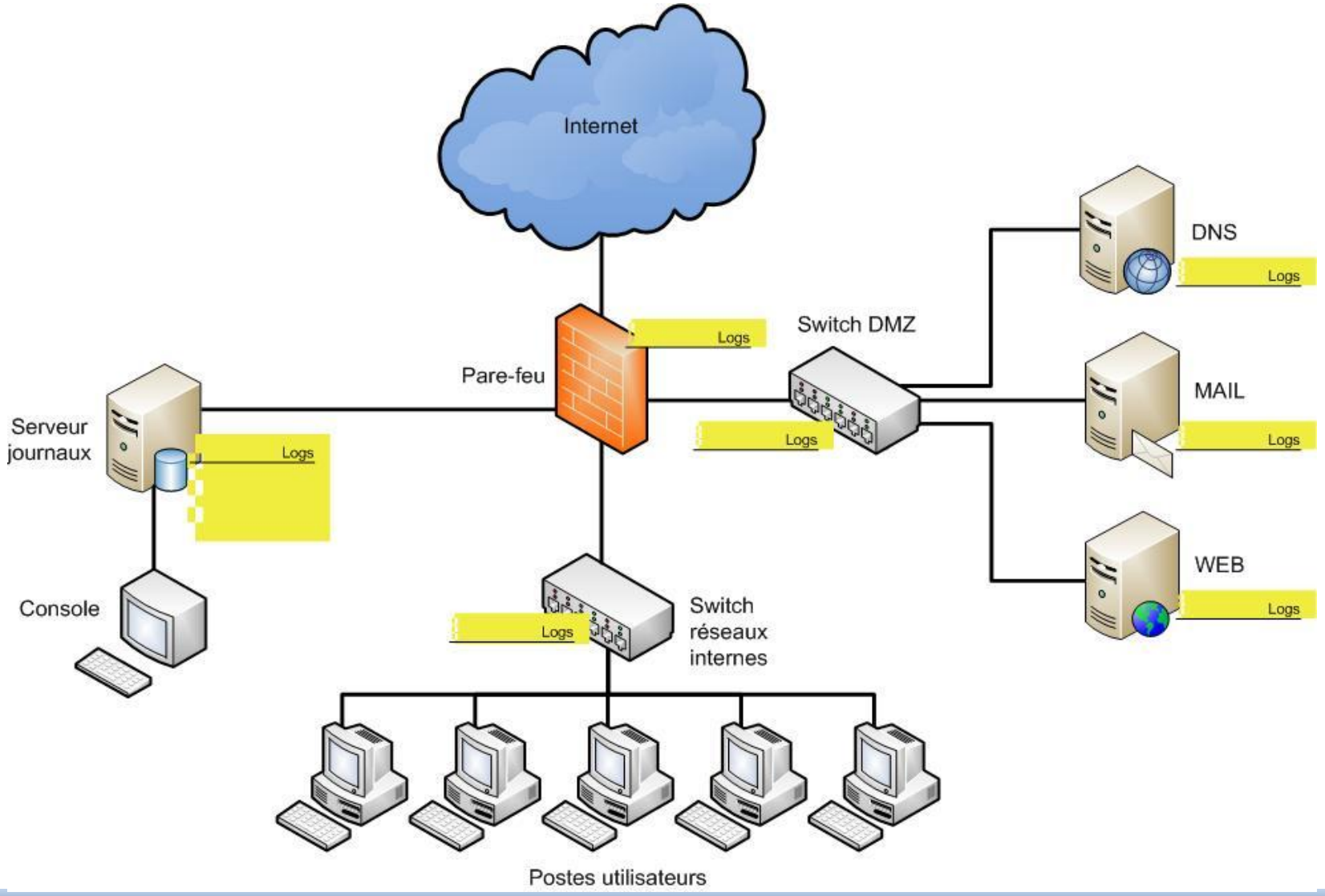
Infrastructure simple



Infrastructure simple

- Capacité de stockage pas toujours adaptée
- Pas d'information fiable si un équipement est compromis
- Peu pratique à l'usage
- Gestion des droits compliquée

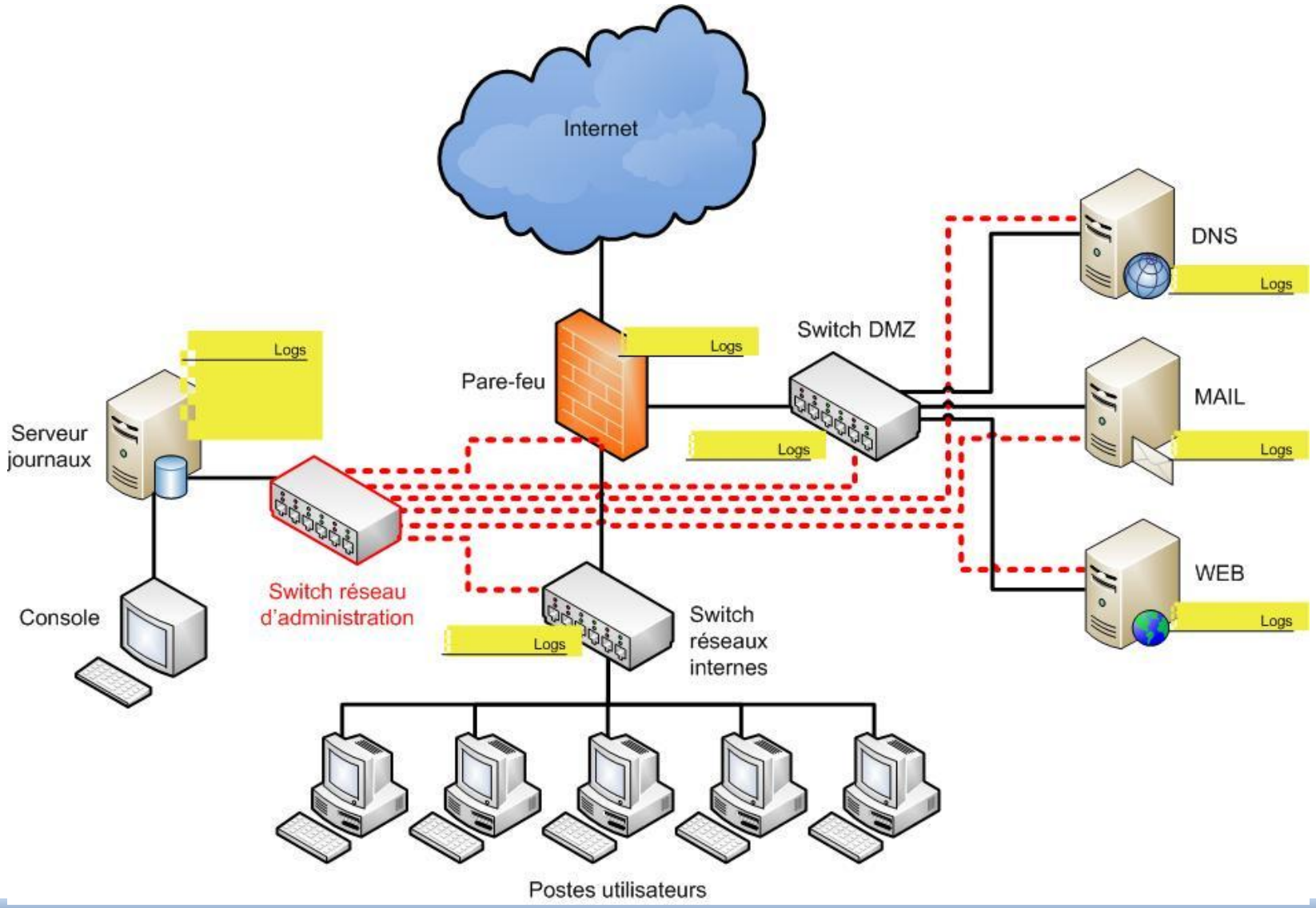
Infrastructure centralisée



Infrastructure centralisée

- Déport des journaux sur une machine isolée
- Chiffrement possible sur le réseau et le serveur de logs
- Capacité de traitement dédiée
- Utilisation d'outils efficaces (base de donnée)
- Dépendant du réseau (bande passante)

Infrastructure centralisée et dédiée



Infrastructure centralisée et dédiée

- Séparation réseaux de production et d'administration : bande passante, interfaces distinctes
- Réseau d'administration peut servir aux sauvegardes, etc.
- Doublement du réseau
- Configuration irréprochable des services réseaux

Virtualisation du serveur de logs

- Machine hôte dédiée aux VM « internes »
- Avantages de la virtualisation
- Capacité de traitement et accès réseau partagés

Exemple de plan d'action

Contrôle et correction au besoin :

- informations qu'il est interdit de journaliser
- données de plus de 1 an, quelque soit le support
- informations qu'il est obligatoire ou conseillé de journaliser
- conservation pendant un an
- centraliser les logs ? mutualiser ?
- droits d'accès
- anonymisation, statistiques

} achat ?

Informer les utilisateurs, la direction