



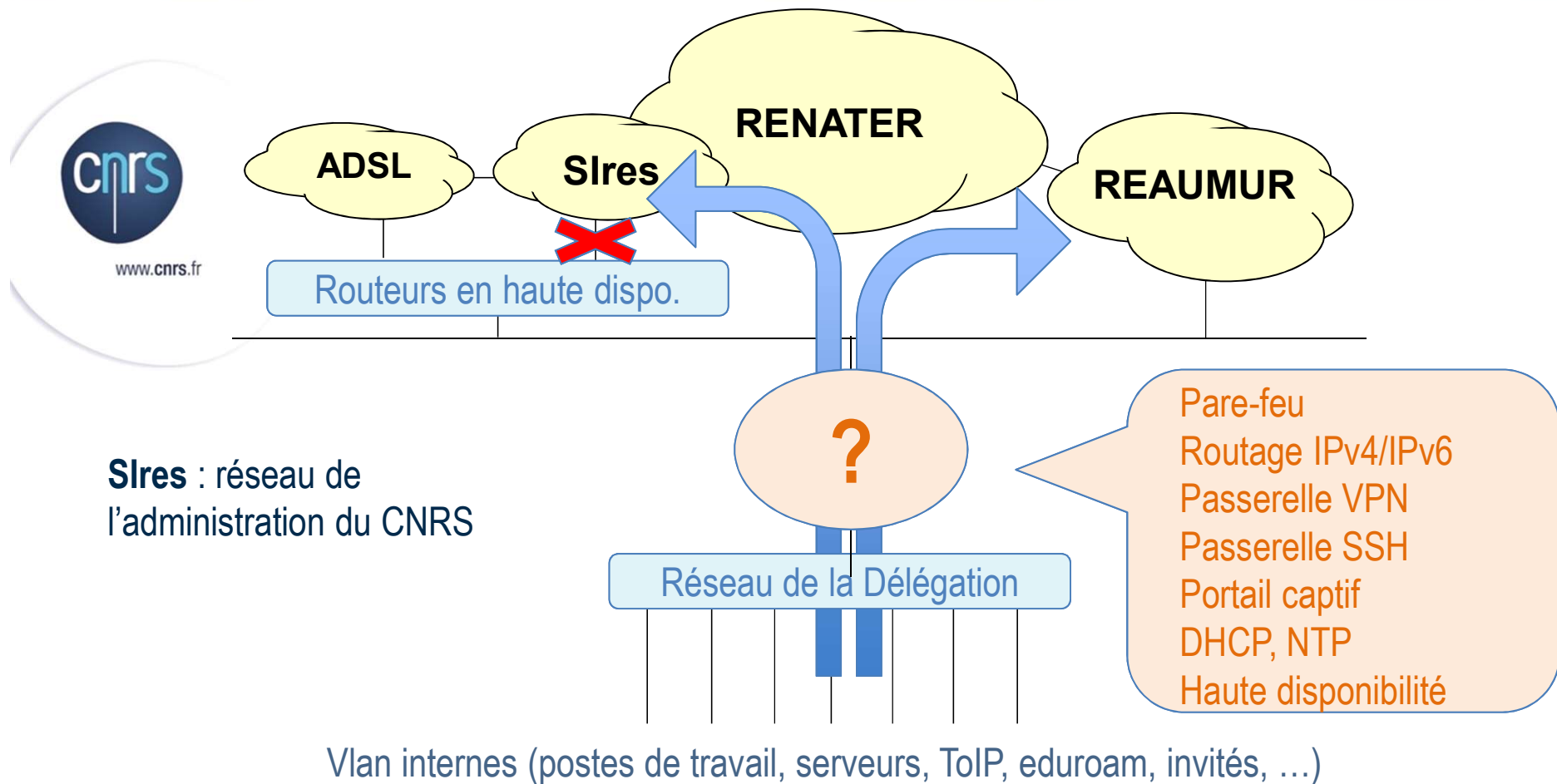
www.cnrs.fr

Retour d'expérience pfSense

Roland Dirlwanger
CNRS Délégation Aquitaine



Le besoin



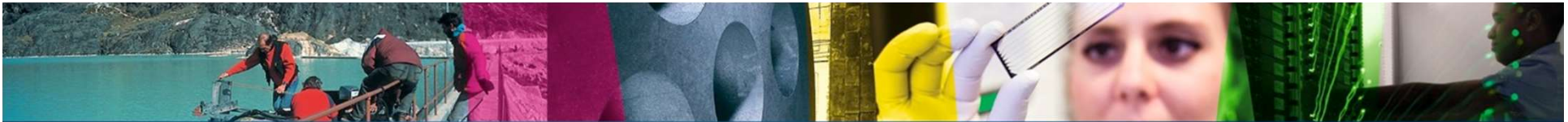


pfSense



- ◎ Choisi en 2014 pour remplacer la solution précédente
 - Routage/Pare-IPv4 par switch L2/L3 Cisco (Catalyst 3650)
 - Routage IPv6 via un serveur Linux

- ◎ pfSense : solution tout en un
 - Basée sur FreeBSD
 - Administrée via une console WWW
 - Interface homogène avec tous les outils classiques du réseau
 - Packet Filter pour la partie Firewall
 - OpenVPN, OpenSSH, DHCP, NTPd, ...
 - Haute disponibilité



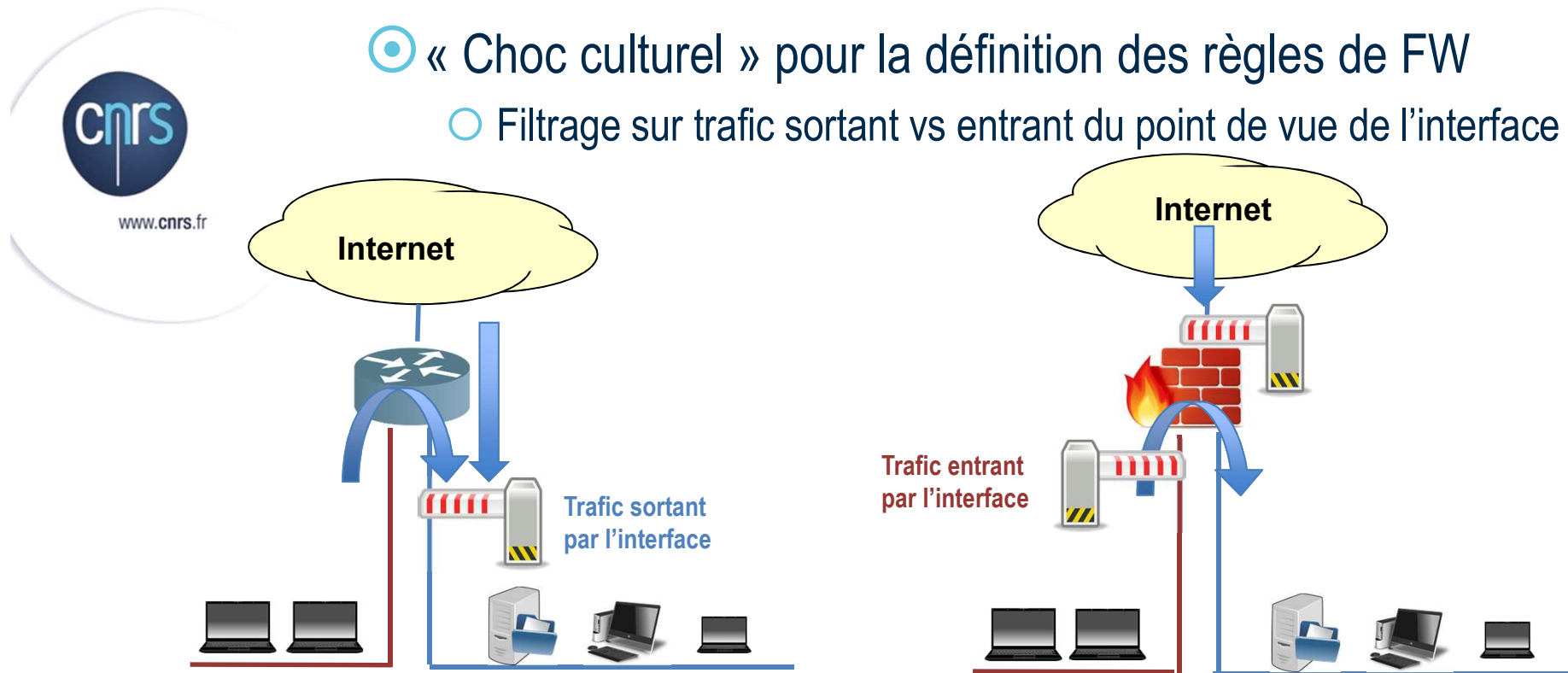
pfSense : les plus



- ⦿ Facile à mettre en œuvre
 - Installation, configuration
 - Mises à jour
- ⦿ Définition des règles facilitées
 - Règles par défaut
 - Règle « inverse » automatique
 - Groupes de machines (alias)
 - Règles communes pour IPv4 et IPv6
- ⦿ Matériel peu onéreux (Dell R220, ~500 €)
- ⦿ Gratuit

pfSense : les moins

- ⦿ « Choc culturel » pour la définition des règles de FW
 - Filtrage sur trafic sortant vs entrant du point de vue de l'interface



- Contourné par l'utilisation de la règle « floating »



Conclusion



- ◎ Solution bien adaptée à notre contexte
 - Quelques centaines d'adresses à filtrer
 - Une dizaine de VLAN
 - Une petite équipe

- ◎ Tient ses promesses
 - Facilité d'administration
 - Haute disponibilité
 - Mises à jour
 - Fiabilité