



Évolution de l'architecture de messagerie

15 septembre 2008

Centre Réseau Communication

Ordre du jour

- 1- Introduction
- 2- Objectifs des changements
- 3- Nouvelle architecture
- 4- Impact et actions nécessaires
- 5- Planning
- 6- Questions

Introduction

- ▶ Changements importants dans le fonctionnement de la messagerie
- ▶ Opération prévue le 30 septembre 2008
- ▶ Impact fort
- ▶ Modifications nécessaires
 - Pour tous les utilisateurs
 - Pour les serveurs de messagerie
 - Pour tout équipement émettant des mails (fax, scanner, onduleurs, etc.)
- ▶ Sans action, le mail ne fonctionnera plus !!!

Ordre du jour

1- Introduction

2- Objectifs des changements

3- Nouvelle architecture

4- Impact et actions nécessaires

5- Planning

6- Questions

Pourquoi ces changements ?

- ▶ Il y a trop de spams émis depuis Osiris
 - Machines piratées
 - Plaintes quotidiennes
 - Osiris en liste noire régulièrement
- ▶ Le port 25 doit être fermé **en sortie**
- ▶ Il faut authentifier les émetteurs de messages
- ▶ L'authentification apporte un nouveau service :
 - Utilisation du serveur SMTP Osiris depuis Internet

Pourquoi ces changements ?

- ▶ Les mots de passe circulent en clair
 - IMAP et POP non sécurisés
- ▶ Chiffrement devenu obligatoire
- ▶ SMTP authentifié requiert le reparamétrage de tous les clients de messagerie
 - C'est l'occasion de passer en IMAPS ou POPS
 - Inutile de modifier deux fois les clients !

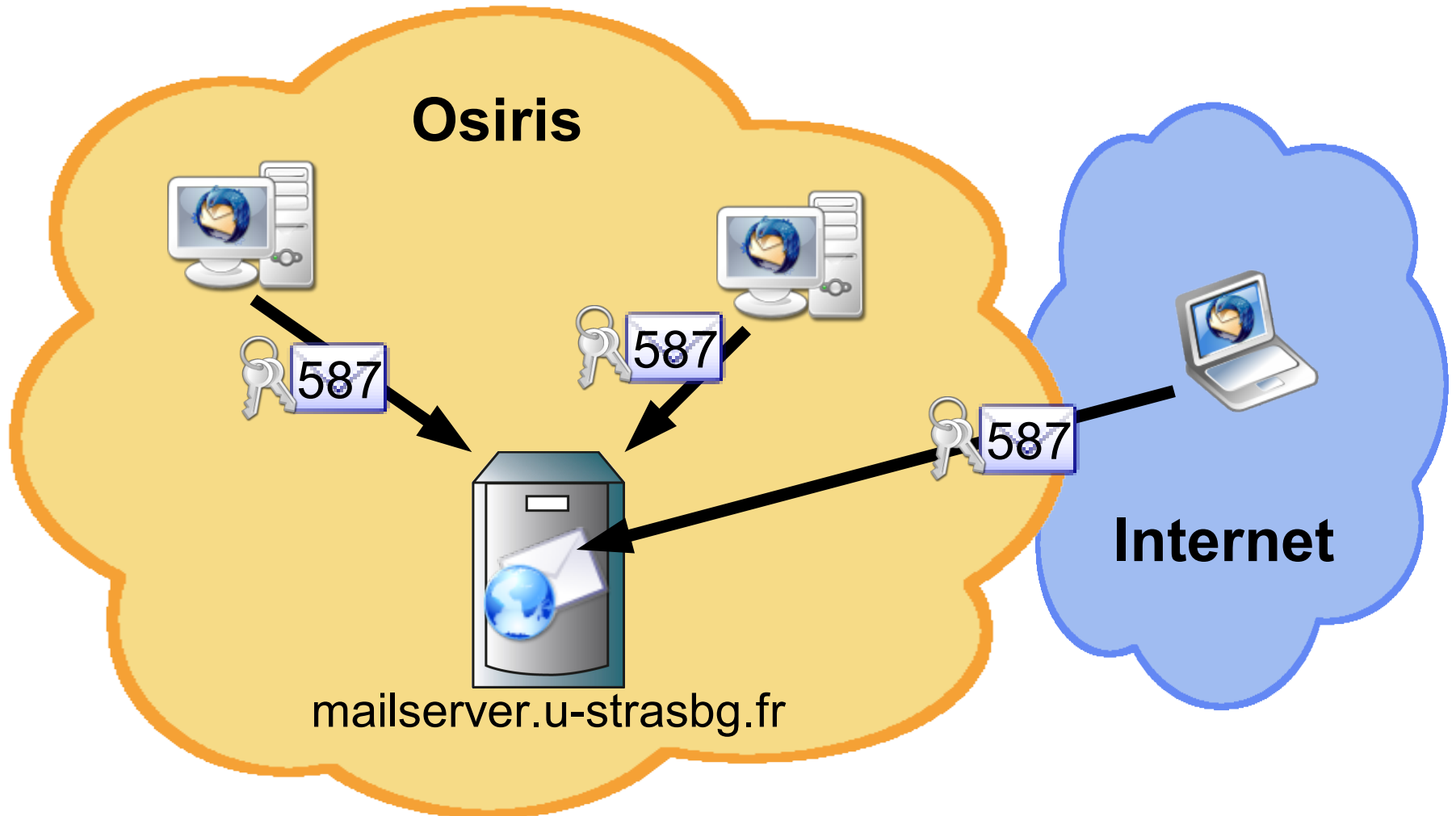
Ordre du jour

- 1- Introduction
- 2- Objectifs des changements
- 3- Nouvelle architecture
- 4- Impact et actions nécessaires
- 5- Planning
- 6- Questions

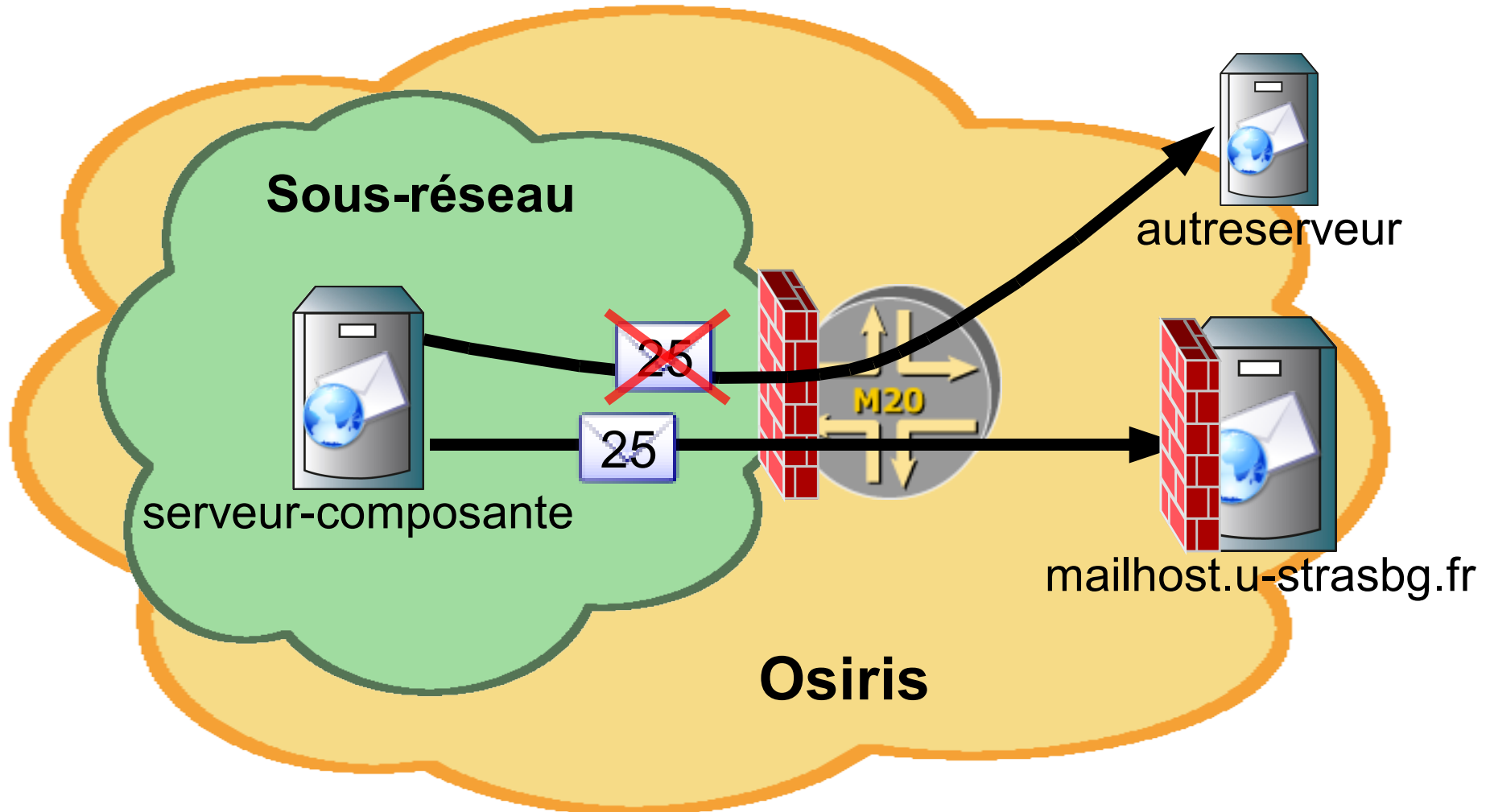
Fermeture de SMTP en sortie

- ▶ Objectif : établir une chaîne de confiance
- ▶ Les utilisateurs doivent s'authentifier
 - sur les serveurs de messagerie du CRC...
 - ... mais aussi sur les autres serveurs de messagerie d'Osiris
- ▶ Seuls les relais Osiris émettent du mail vers Internet
- ▶ Doivent passer par les relais
 - Les serveurs de mails identifiés comme tels
 - Les autres exceptions (copieurs, applications)
- ▶ Ce relayage SMTP est autorisé via WebDNS

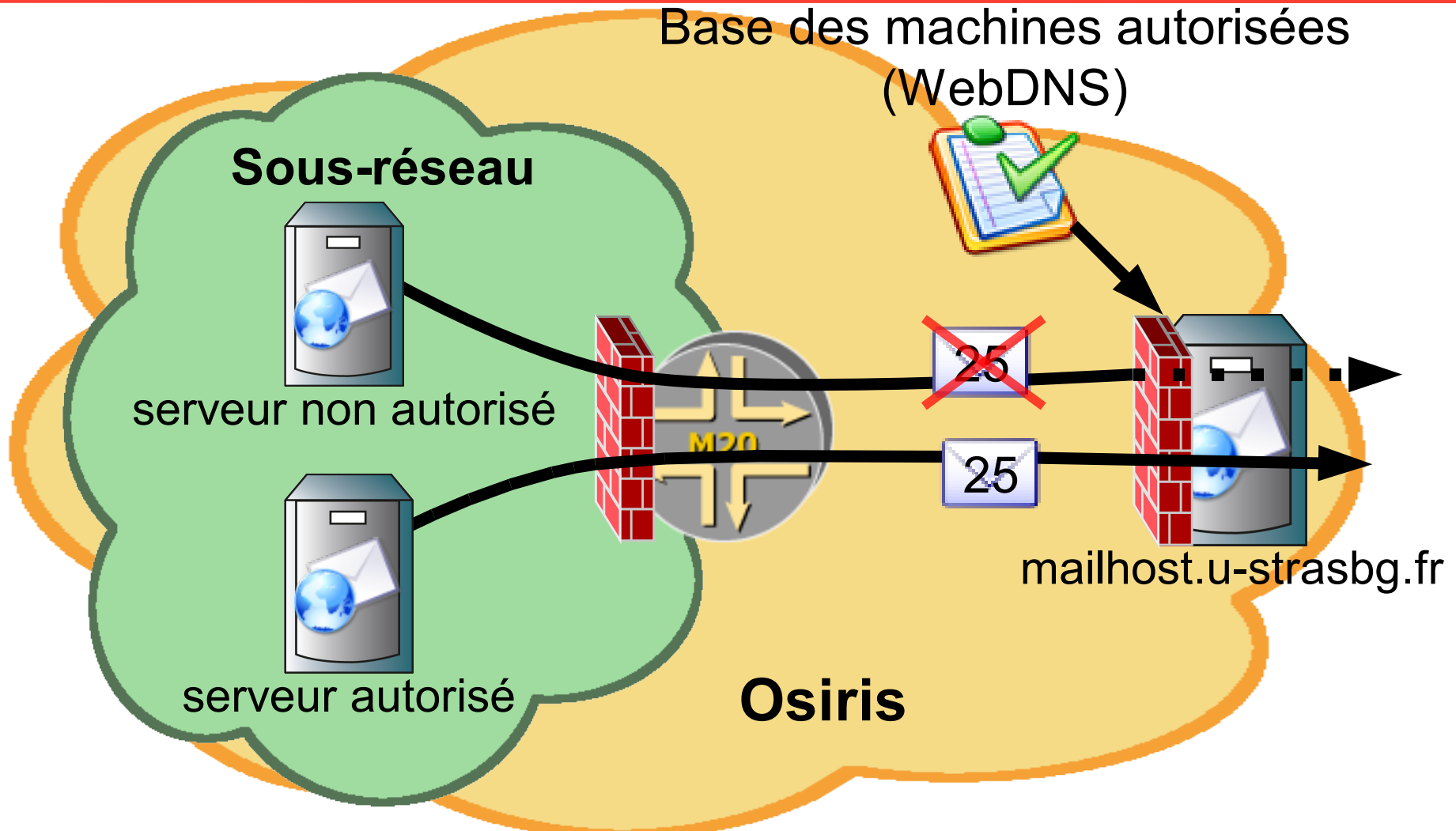
Émission par les clients



Filtrage en sortie de sous-réseau



Filtrage sur les relais Osiris



Arrêt de POP et IMAP non sécurisés

- ▶ Sur ces services le mot de passe circule en clair
- ▶ le 30 septembre, les services suivants seront arrêtés :
 - IMAP : port 143
 - POP3 : port 110
- ▶ Les clients devront utiliser leurs équivalents sécurisés (SSL) :
 - IMAPS : port 993
 - POP3S : port 995

Ordre du jour

- 1- Introduction
- 2- Objectifs des changements
- 3- Nouvelle architecture
- 4- Impact et actions nécessaires
- 5- Planning
- 6- Questions

Impact immédiat

- ▶ Au 30 septembre, si rien n'est fait :
 - Les utilisateurs ne pourront plus envoyer de messages
 - Les utilisateurs en POP et IMAP non sécurisé n'accèdent plus à leur boîtes aux lettres
 - Les mails émis par les serveurs sans passer par les relais Osiris seront bloqués
 - Les mails émis par les serveurs non autorisés dans WebDNS seront bloqués

Actions pour les utilisateurs

- ▶ Reconfigurer les logiciels de messagerie
 - serveur de courrier entrant
 - serveur SMTP sortant
- ▶ Procédures disponibles :
 - <http://www-crc.u-strasbg.fr/osiris/services/bal>
- ▶ Remarque : versions « anciennes » d'Outlook et d'Eudora
 - Ne peuvent pas utiliser le port 587 en TLS
 - Ouverture d'un service SMTPS sur le port 465
 - À n'utiliser que si le port 587 n'est pas supporté !!!

Actions pour les exceptions

- ▶ Qu'est ce qu'une exception ?
 - Une machine hébergeant une application émettant des messages
 - Un fax, un copieur, un onduleur, etc. émettant des mails
- ▶ Garantir que cette machine n'effectue pas de relayage : le port 25 doit être fermé
- ▶ Configurer un relais de messagerie
 - mailhost.u-strasbg.fr
- ▶ Autoriser la machine à émettre dans WebDNS
 - Cocher la case « Émettre en SMTP »

Actions pour les serveurs de messagerie

- ▶ Garantir que cette machine n'est pas un relais ouvert :
 - Authentification obligatoire pour tous les utilisateurs
 - le port 25 ne sera plus accessible hors du sous-réseau : utiliser le port 587
- ▶ Configurer un relais de messagerie
 - mailhost.u-strasbg.fr
- ▶ Autoriser la machine à émettre dans WebDNS
 - Cocher la case « Émettre en SMTP »

Actions pour les serveurs de messagerie

- ▶ Garantir que cette machine n'est pas un relais ouvert :
 - Authentification obligatoire pour tous les utilisateurs
 - le port 25 ne sera plus accessible hors du sous-réseau : utiliser le port 587
- ▶ Configurer un relais de messagerie
 - mailhost.u-strasbg.fr
- ▶ Autoriser la machine à émettre dans WebDNS
 - Cocher la case « Émettre en SMTP »

Ordre du jour

- 1- Introduction
- 2- Objectifs des changements
- 3- Nouvelle architecture
- 4- Impact et actions nécessaires
- 5- Planning
- 6- Questions

Planning

- ▶ 16/07 : SMTP authentifié sur mailserver.u-strasbg.fr
- ▶ 01/09 : Autorisation SMTP dans WebDNS
- ▶ Jusqu'au 30 septembre :
 - Test opérationnel : activation du filtrage sur votre demande
 - Recommandé : éviter les surprises et l'affluence du 30/09
- ▶ 30 Septembre 2008:
 - Mise en place du filtrage du port 25 pour tous les réseaux
 - Fermeture des services POP et IMAP non-sécurisés

▶ Questions ?