

Le Groupe des Utilisateurs en sécurité Microsoft de Montréal présente



<http://www.gusmm.org>

Exchange 2003
Sécurité et meilleures
pratiques

Exchange 2003

Sécurité et meilleures pratiques

- Frédéric Asselin
- Conseiller Senior - Associé chez Loran Technologie
- V-P Groupe des Utilisateurs en sécurité Microsoft de Montréal
- fred@lorantech.com



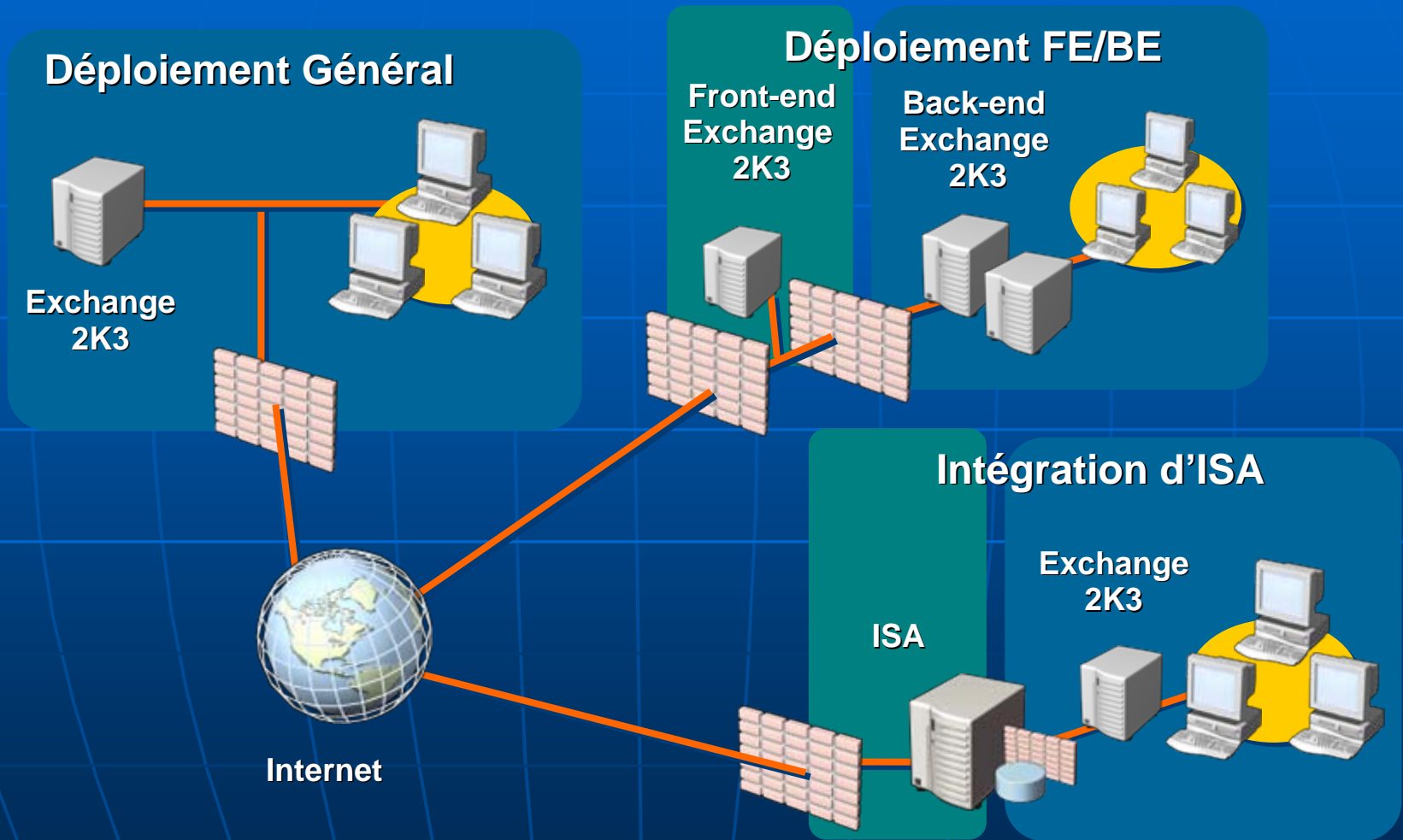
Agenda

- Mot de bienvenue
- Modèles d'implantation Exchange 2003
- Sécurisation des service et protocoles
- Maintien de la sécurité pour Exchange 2003
- Protection contre le courrier indésirable
- Accès et privilèges

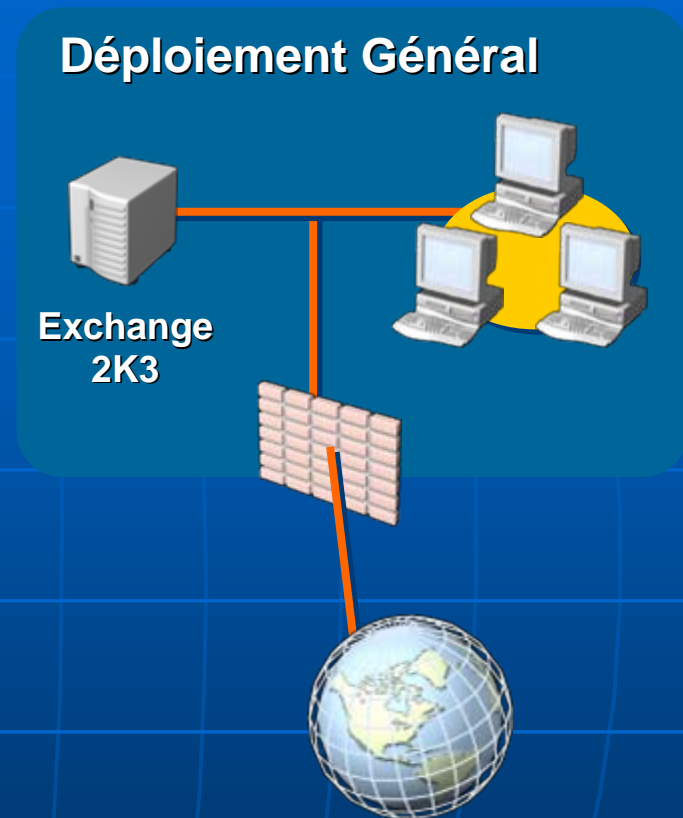
Implantation d'Exchange 2003

- Sécuritaire par design
 - Support pour :
 - ✓ *Sender filtering*
 - ✓ *Recipient filtering*
 - ✓ *Connection filtering,*
 - ✓ *Block List services*
- Sécuritaire par défaut
 - Enregistrement local désactivé
 - Limite de 10MB pour les messages

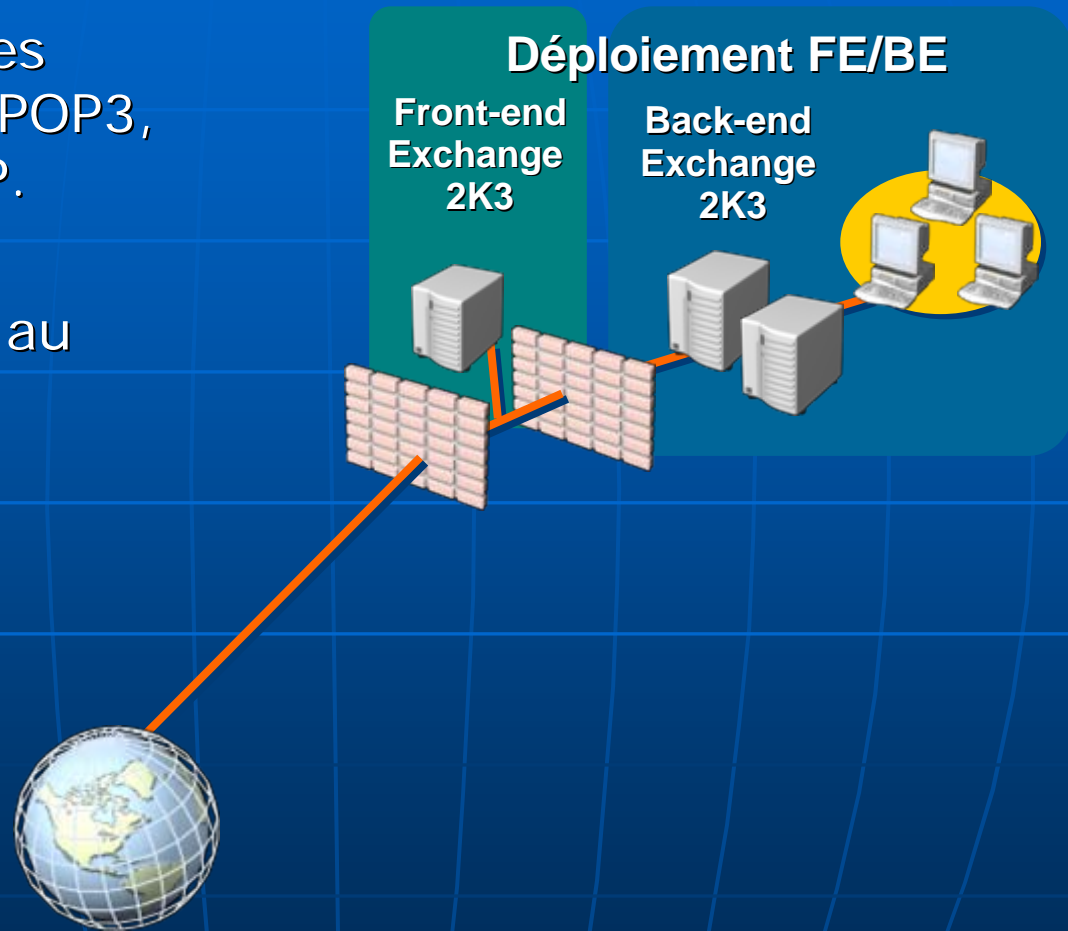
Scénarios de déploiement Exchange 2003



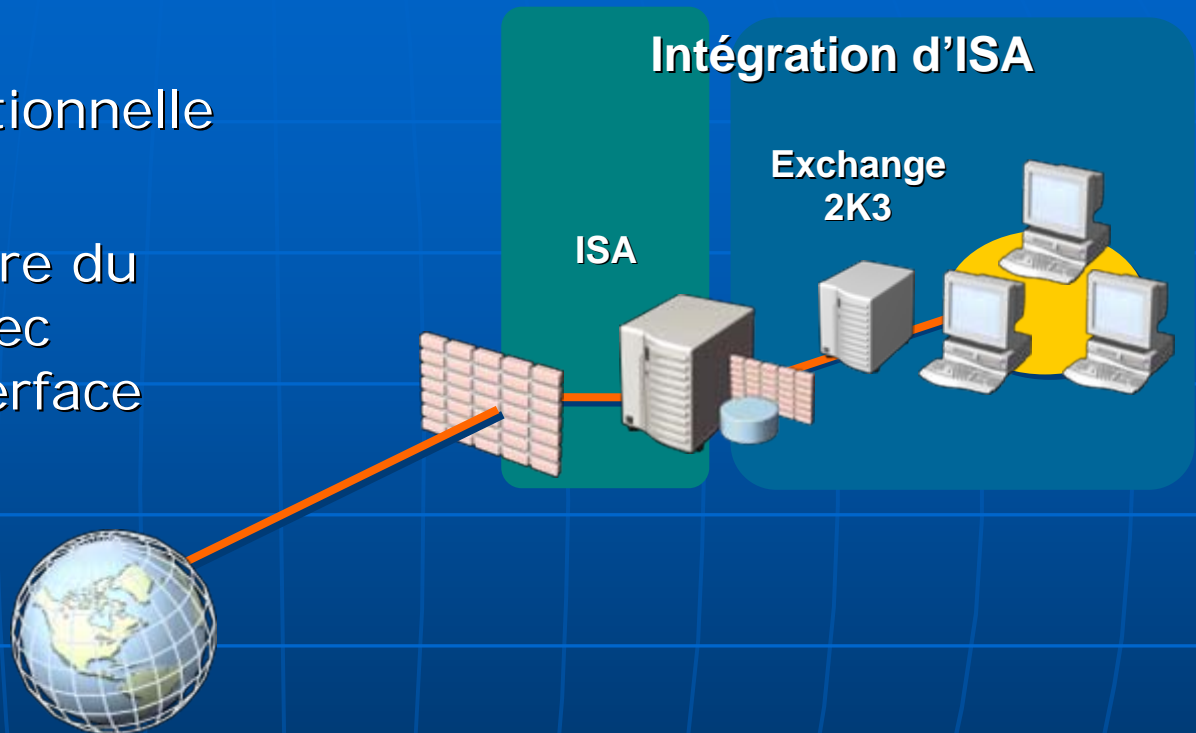
- Généralement pour les organisation plus petites
- Les relais SMTP sont sur une autre plate forme
- Pas besoin d'Outlook Web Access



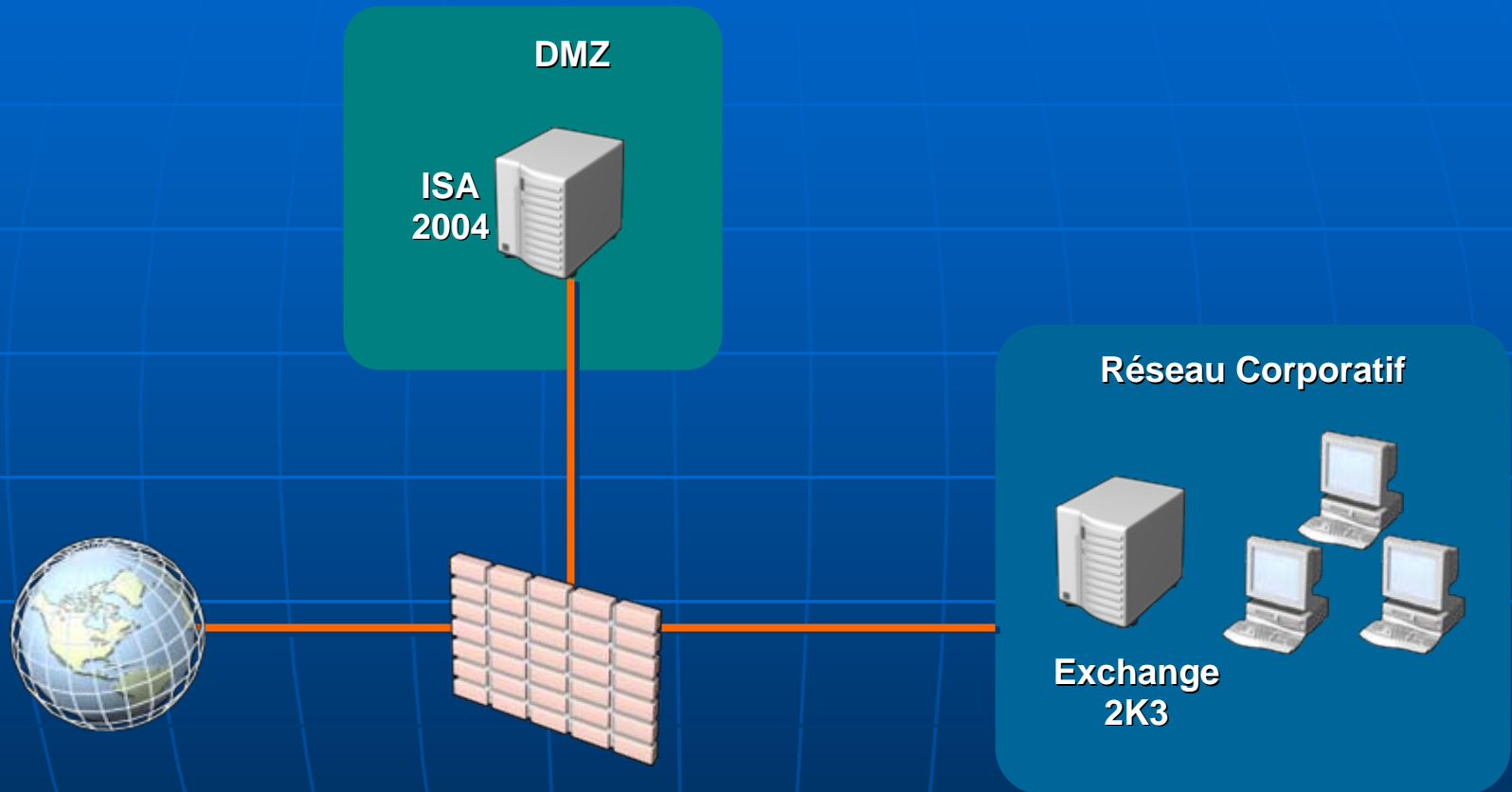
- Plusieurs protocoles Internet utilisés : POP3, HTTP, IMAP, SMTP.
- Pas d'accès direct au périmètre interne



- Sécurisation additionnelle
- ISA 2004 peut faire du Reverse Proxy avec seulement un interface réseau



ISA 2004 Reverse Proxy



Mise à jour des correctifs de sécurité et recommandations

Composantes	Configuration
Système d'exploitation et logiciels	<ul style="list-style-type: none">• Microsoft Windows Server 2003 à jour aux derniers correctifs de sécurité• Exchange Server 2003 avec Service Pack 1 (et plus...)• Microsoft Exchange Intelligent Message Filter• Antivirus à jour à la dernière signature
Fureteur	<ul style="list-style-type: none">• Internet Explorer 6 à jour avec les derniers correctifs de sécurité
Mise à jour de la sécurité	<ul style="list-style-type: none">• Microsoft Baseline Security Analyzer• ExBPA

Sécurisation des service et protocoles pour Exchange 2003

- Quels sont les défis ?
 - Maintenir la sécurité du système d'exploitation
 - Maintenir les paramètres de sécurité implantés pour Exchange 2003
 - Bien comprendre les diverses options de sécurité selon le scénario de déploiement retenu.

Renforcement de la sécurité pour Exchange 2003

Environnement	Configuration
Environnement Serveur	<ul style="list-style-type: none">·Domaine, Contrôleur de domaine et serveur membre stratégie de sécurité.·Windows Server 2003 Security Guide http://go.microsoft.com/fwlink/?LinkId=21638
Exchange 2003	<ul style="list-style-type: none">·Exchange Domain Controller Baseline Policy template·Exchange Serveur 2003 Security Hardening Guide http://www.microsoft.com/technet/prodtechnol/exchange/2003/library/exsecure.mspx

Sécurisation des serveurs dorsaux (back-end)

- Tâches pour sécuriser les serveurs dorsaux
 - Sécurisation des services
 - Sécurisation des accès (ACLs)
 - Gestion des privilèges
- Appliquer la stratégie Backend.inf
- Voir Exchange 2003 Hardening Guide

Sécurisation des serveurs frontaux (front-end)

- Tâches pour sécuriser les serveurs frontaux
 - Sécurisation des services
 - Sécurisation des accès (ACLs)
 - Gestion des privilèges
 - Utiliser URLScan (optionnel) KB → 823175
 - Démonter les bases de données de boîtes aux lettres et détruire les bases de données de dossiers publics (optionnel)
- Appliquer la stratégie Frontend.inf et la stratégie selon le service offert
- Voir Exchange 2003 Hardening Guide

Démonstration

Importation de gabarits de
sécurité

Comprendre le routage SMTP

- **Le routage SMTP est nécessaire quand :**
 - Vous gérer plusieurs noms de domaine SMTP
 - Vous supportez des clients POP3 et IMAP
 - Vous supporter des applications qui utilisent SMTP
- **Prévenir le routage SMTP :**
 - Permettre le routage a des ordinateurs authentifiés
 - Restreindre le routage SMTP à des clients spécifiques
 - Utiliser des connecteurs pour diriger le courrier à des nom de domaines particuliers

Vérification de relais ouvert ...

www.ordb.org

This host is not listed in ORDB as an open mail relay

Main database status for **gusmm.org**
(206.123.35.190) Look up this host in non-ORDB RBL's (May take a while to load) The host gusmm.org is not in the main database

Queue status for **gusmm.org**
(206.123.35.190) The host gusmm.org is not queued for testing at this time You may schedule a retest of gusmm.org by clicking here

Meilleures pratiques

- Limiter les fonctionnalités d'Exchange 2003 selon les besoins de vos clients
- Mettre à jour les service pack et les correctifs de sécurité, Exchange 2003 et Windows 2003
- Utiliser ISA pour gérer le trafic de vos protocoles Internet ...
- Utiliser un certificat SSL et l'authentification *forms-based* pour Outlook Web Acces ...

Maintien de la sécurité

- Les défis pour Exchange 2003 sont :
 - Les correctifs de sécurité
 - Les meilleures pratiques
 - Comprendre les configurations possibles
 - Maintenir les configurations ...

Security Configuration Wizard

Le Security Configuration Wizard de Windows 2003 Serveur sp1, inclut un profil Exchange 2003.

Attention ... !

Démonstration

Security Configuration Wizard

MBSA

- MBSA va identifier pour vous :
 - Les risques pour Windows et Internet Explorer
 - Les correctifs de sécurité manquants
 - Les risques pour IIS
 - Les risques pour Exchange

EXBPA

Exchange Best Practices Analyser

- EXBPA vous fournit de l'information sur :
 - Les configurations erronées et non supportées
 - *Health Check* d'Exchange
 - Peut servir à solutionner des problèmes dans votre infrastructure Exchange

Démonstration

Exchange Best Practice
Analyser

Antivirus

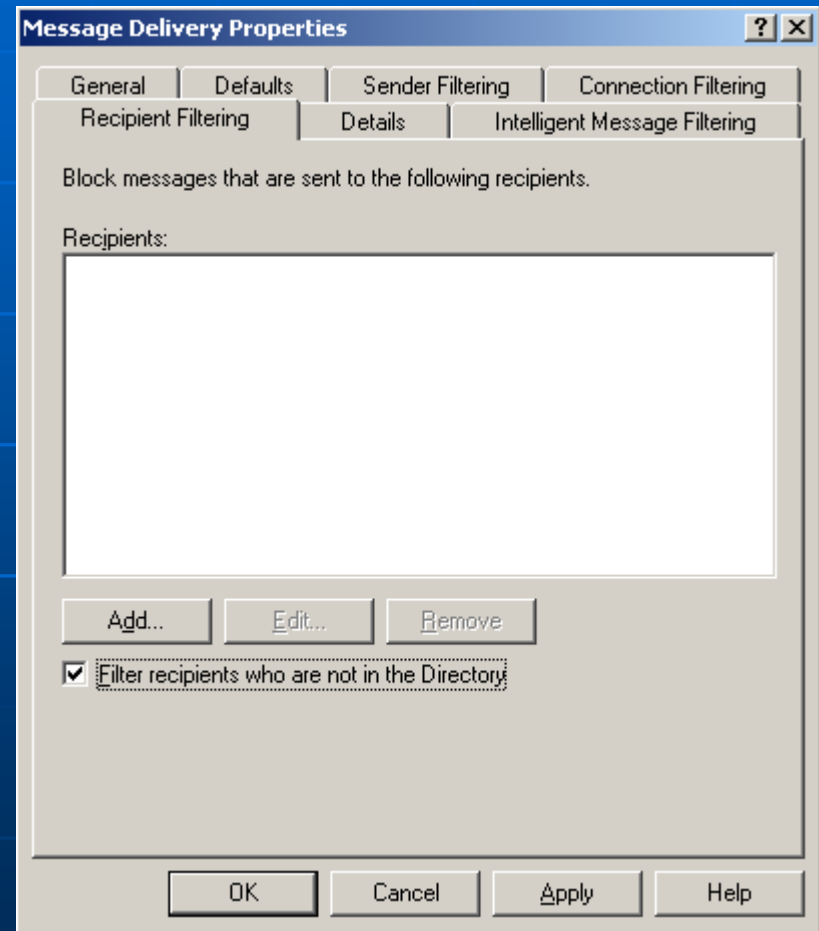
- Utilisation de AVAPI 2.5
KB → 823166
- Sécuriser toutes les serveurs
Exchange de votre infrastructure
- Ne pas *scanner* les fichiers Exchange
avec un antivirus de fichiers

Protection contre le courrier indésirable

- Options :
 - Recipient filtering
 - Sender filtering
 - Connection filtering
 - Microsoft Exchange Intelligent Message Filter
 - Logiciel tiers

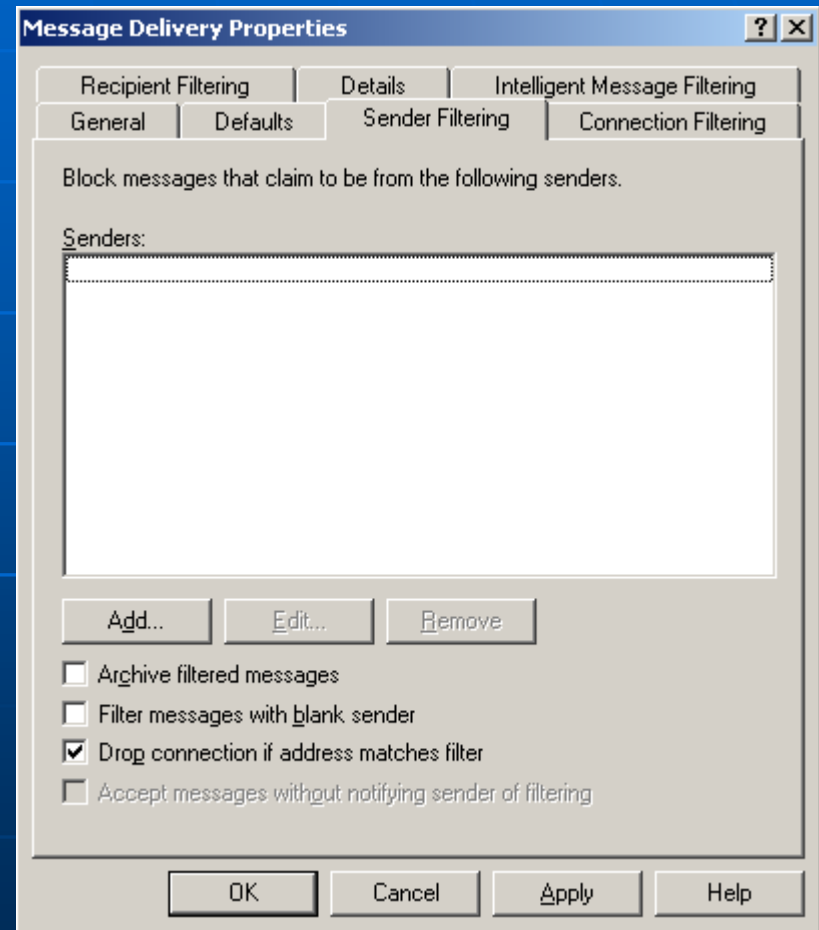
Recipient Filtering

- Bloque les messages envoyés au destinataires de votre domaine de votre choix
- Filtre les destinataires de votre domaine qui ne sont pas dans votre Active Directory
Attention ...



Sender Filtering

- Bloque les messages des envoyeurs de votre choix ou de noms de domaine

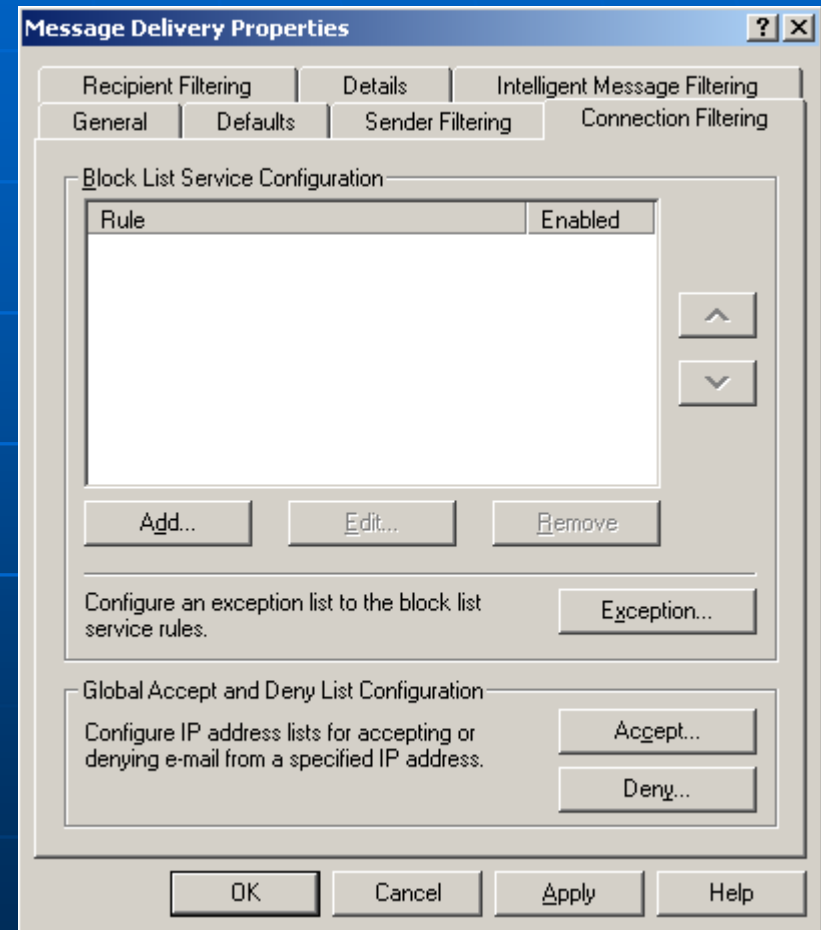


Connection Filtering

- Exchange peut utiliser un *Real Time Block List* pour bloquer les emails non désirés

Relays.ordb.org

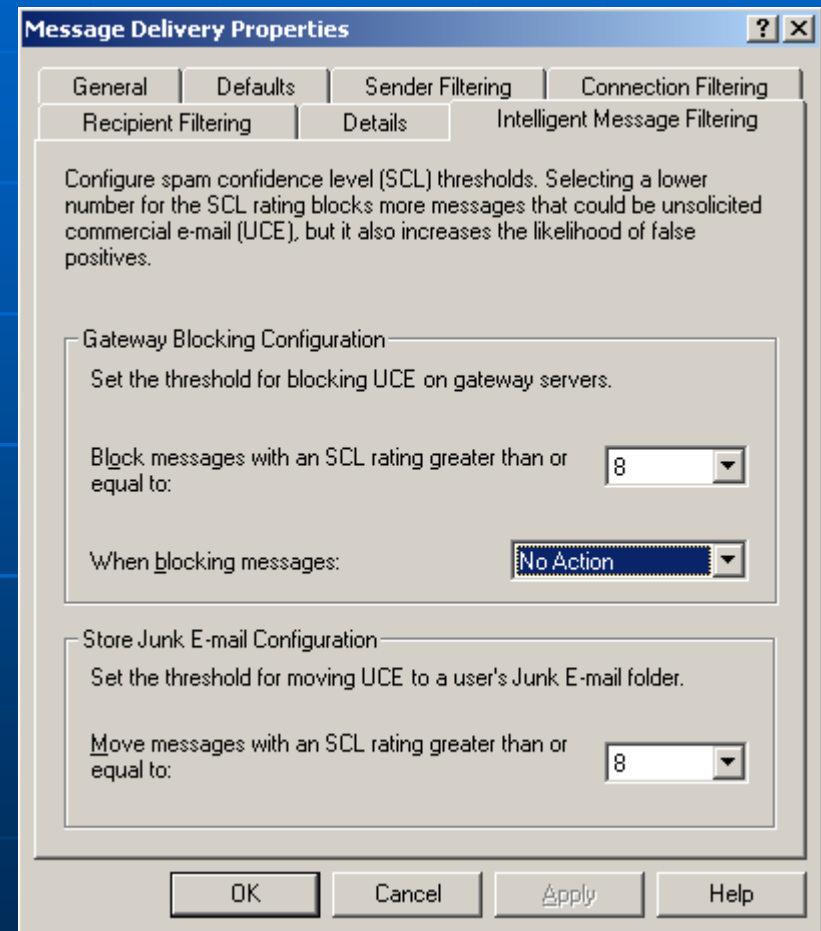
http://www.msexchange.org/tutorials/Blacklist_Support_Exchange_2003.html



Intelligent Mail Filtering

- Ajout gratuit de Microsoft pour bloquer le courrier indésirable
- Outil pour gérer les courriers bloqués

<http://www.msexchange.org/tutorials/microsoft-exchange-intelligent-message-filter.html>



Démonstration

Sender Filtering

Connection Filtering

Recipient Filtering

Intelligent Mail Filtering

Accès et privilèges

3 types de rôles dans Exchange 2003

- Exchange Administrateur Intégral
- Exchange Administrateur
- Exchange Administrateur lecture seulement

Accès et privilèges

Pour plus de granularité dans Exchange System Manager, vous pouvez voir l'onglet sécurité en ajoutant un clef de registre

- **HKEY_CURRENT_USER\Software\Microsoft\Exchange\ExAdmin**
- On the **Edit** menu, click **Add Value**, and then add the following registry value:
- Value Name : **ShowSecurityPage**
- Data Type : **REG_DWORD**
- Value : **1**

EDSlock.vbs

Le groupe Domain Exchange Servers a accès à toutes les bases de données de la forêt.

EDSlock.vbs restreint l'accès aux serveurs Exchange seulement.

Article du KB Microsoft 313807

DSACLS.EXE

Utilitaire de Windows Support Tools pour gérer les ACL des objets et attributs de votre Active Directory

Exemples :

- Modifier le droit en écriture sur l'attribut de l'adresse email
- Modifier le droit de déplacer les boites aux lettres

Article du KB Microsoft 281146

Démonstration

DSACLs

Quelques liens intéressants

<http://www.msexchange.org/>

<http://www.microsoft.com/technet/prodtechnol/exchange/2003/secure.mspx>

<http://www.exchangeserver2003.com>

<http://www.slipstick.com/>

<http://www.ordb.org/>



Merci !