Sybari Software

Gordana Cindric
Consultante Avant-Vente
gordana_cindric@sybari.com

Sybari Software

- **DEC-94**: Début du développement d'Antigen for Lotus Notes
- **NOV-96**: McAfee distribue Antigen v3.0 sous le nom de GroupShield
- **JUN-97**: Sybari commence le développement d'une solution sous Exchange basé MAPI
  - Beta seulement, produit jamais distribué
- **AUG-97**: Début du développement d'Antigen v5.0 for Exchange
- **DEC-98**: Antigen v5.0 for Exchange version finale
- **AUG-99**: Antigen v5.5 for Exchange (ajoutant l'analyse sur IMC)
- **OCT-99**: Microsoft Exchange Conference (MEC)- "Best of Show"
- **NOV-99**: Antigen v5.5 SR1 (ajoutant la fonction de File Filtering)
- **DEC-99**: Compaq White paper
- **JAN-00**: Sybari Europe
- **JUN-00**: Annonce du support de Microsoft sur le logiciel Antigen Exchange
- **OCT-00**: Antigen 6.0 (Exchange 2000 support)
- **MAY-01**: Antigen 6.1 (Option de Purge)
- **JUN-01**: TechED- "Best of Show" dans la catégorie Exchange 2000
- **JUL-01**: Antigen 6.0 for Domino R4/R5
- **AUG-01**: Antigen 6.2 (double mode de fonctionnement ESE / VSAPI 2.0)
- **MAR-02:** Antigen 6.5 (Filtrage par sujet/émetteur/nom de domaine)

Présence internationale

Bureaux

- Amérique du Nord: New York ***(Siège social)***
- Amérique du Sud: Sao Paolo
- Asie: Sidney, Singapour, Inde
- Moyen-Orient: Dubai
- Europe: Madrid ***(Siège européen)***
  Londres
  Rome
  Paris
  Amsterdam
  Munich

Support Technique

- Madrid (24/7): Anglais, Allemand, Espagnol, Français, Néerlandais, Suédois...
- New York (24/7) et San Jose
- Singapour

Références

- Akzo Nobel - Holland
- Airbus Industrie – France
- BBC Worldwide – UK
- Bank of Austria – Austria
- Bosch Siemens – Germany
- Commerzbank - Germany
- Compaq Computers – USA
- Dell Computers – USA
- Deloitte & Touche - USA
- DSM – Holland
- EMC – USA
- EMI Recorded Music – UK
- Ericsson – Sweden
- European Union – Belgium
- Getronics – USA
- Glaverbel – Belgium
- Interbrew – Belgium
- KPN – Holland
- Libertel - Holland
- London Underground – UK
- Lufthansa - Germany
- Mannesmann – Germany
- Merrill Lynch – USA
- Nortel Networks – Canada
- NOVO Nordisk – Norway
- Pentagon – USA
- Pirelli - Italy
- Poste Italia – Italy
- Rabobank – Holland
- SAS - Denmark
- Skandia – Sweden
- Société Générale – France
- Telecom Italia - Italy
- Telia - Sweden
- Texaco – USA
- Tractebel – Belgium
- US House of Representatives
- VISA – USA
- Vodafone – UK

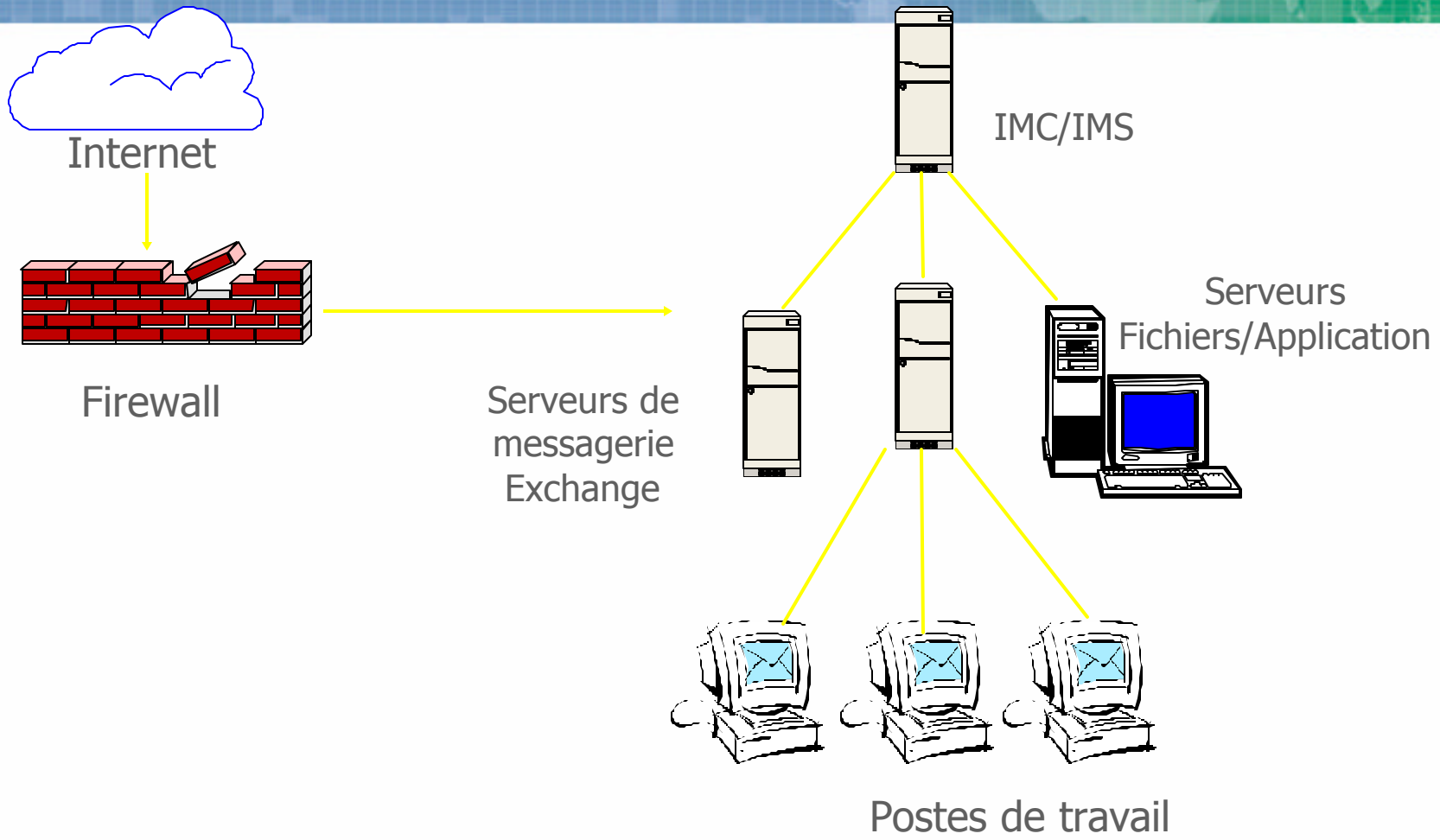
Antigen
High-Performance Groupware Security

Strategies Anti-virales:

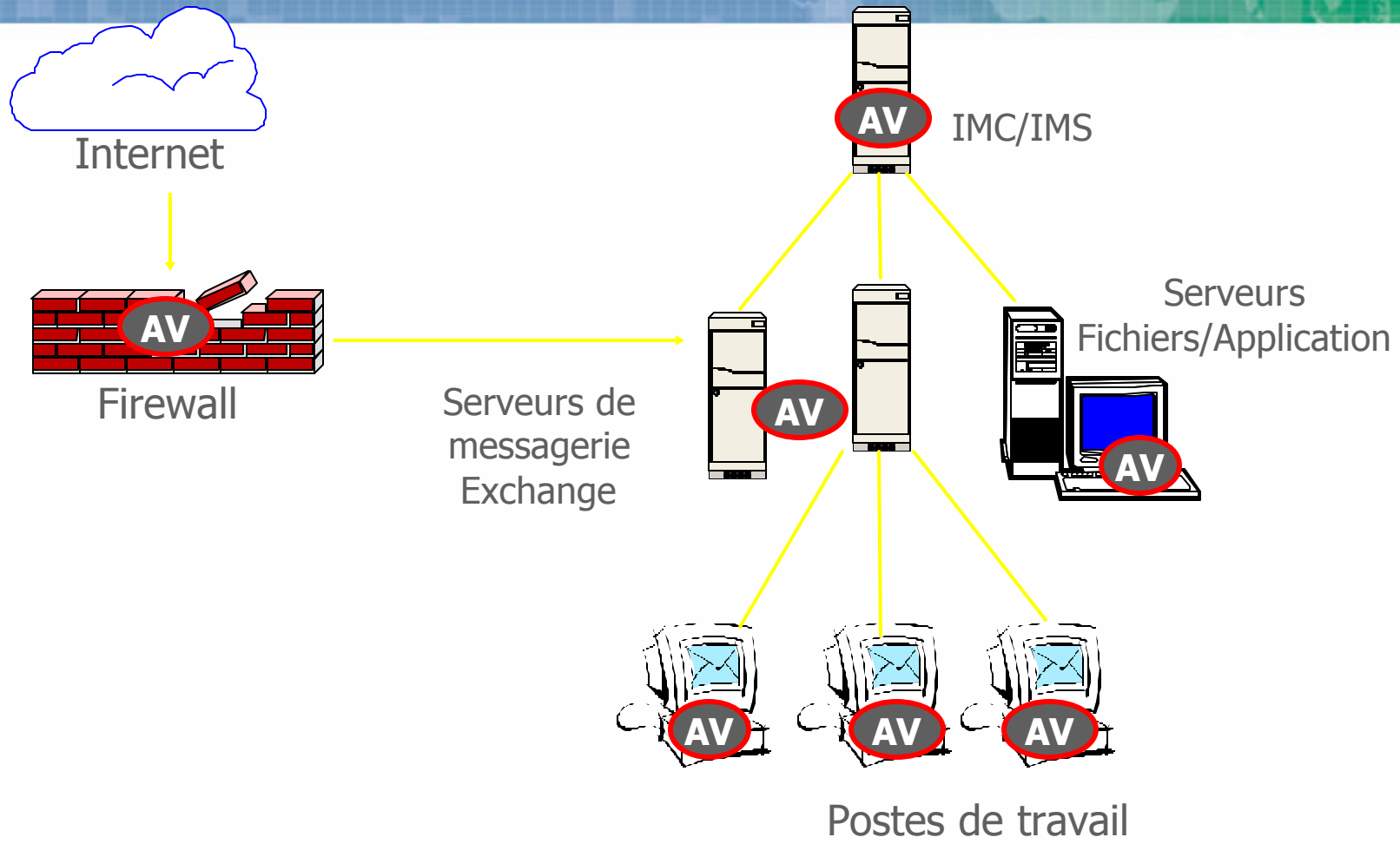
Périmètre de sécurité

Sybari
Ever-Vigilant Protection

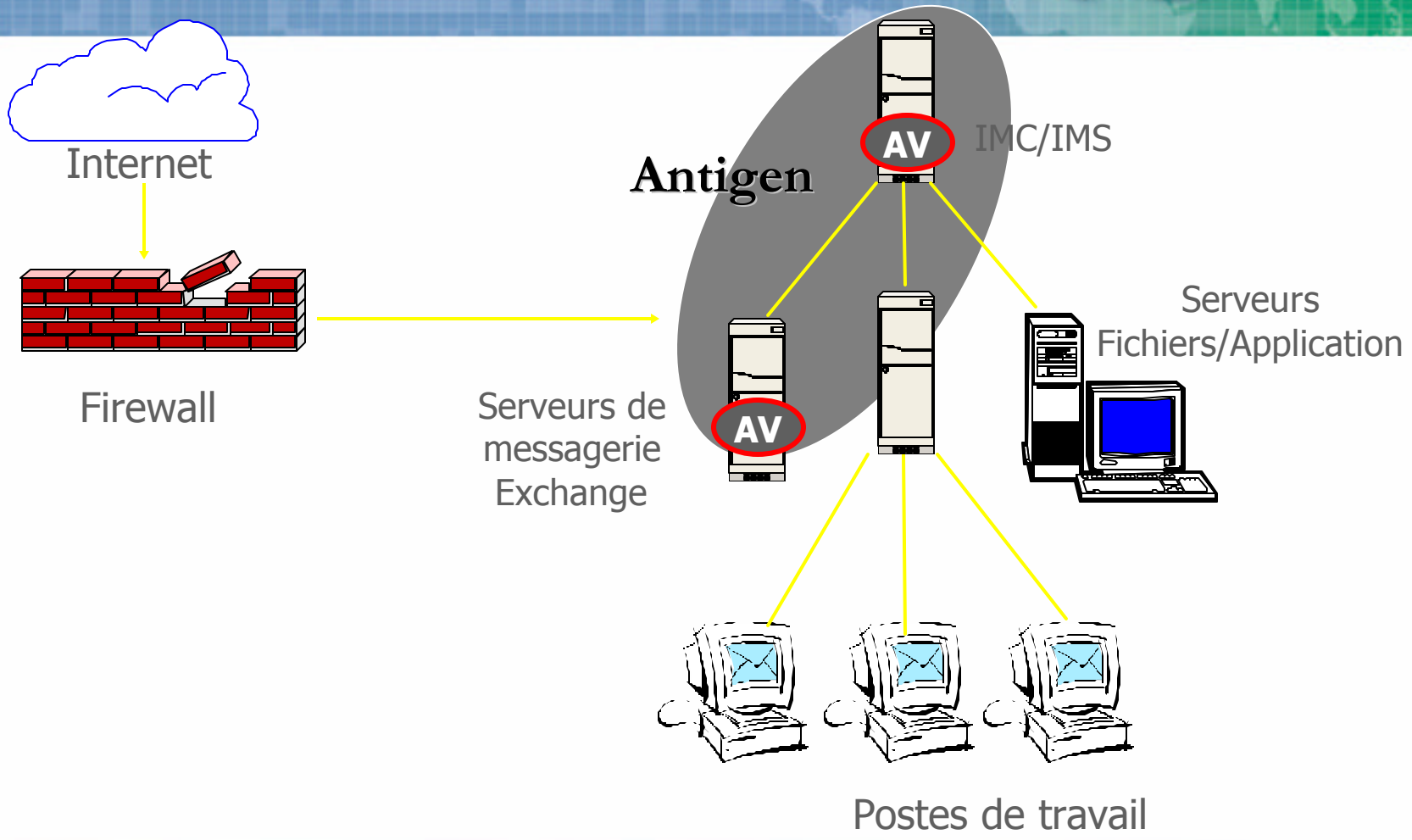
Périmètre de sécurité



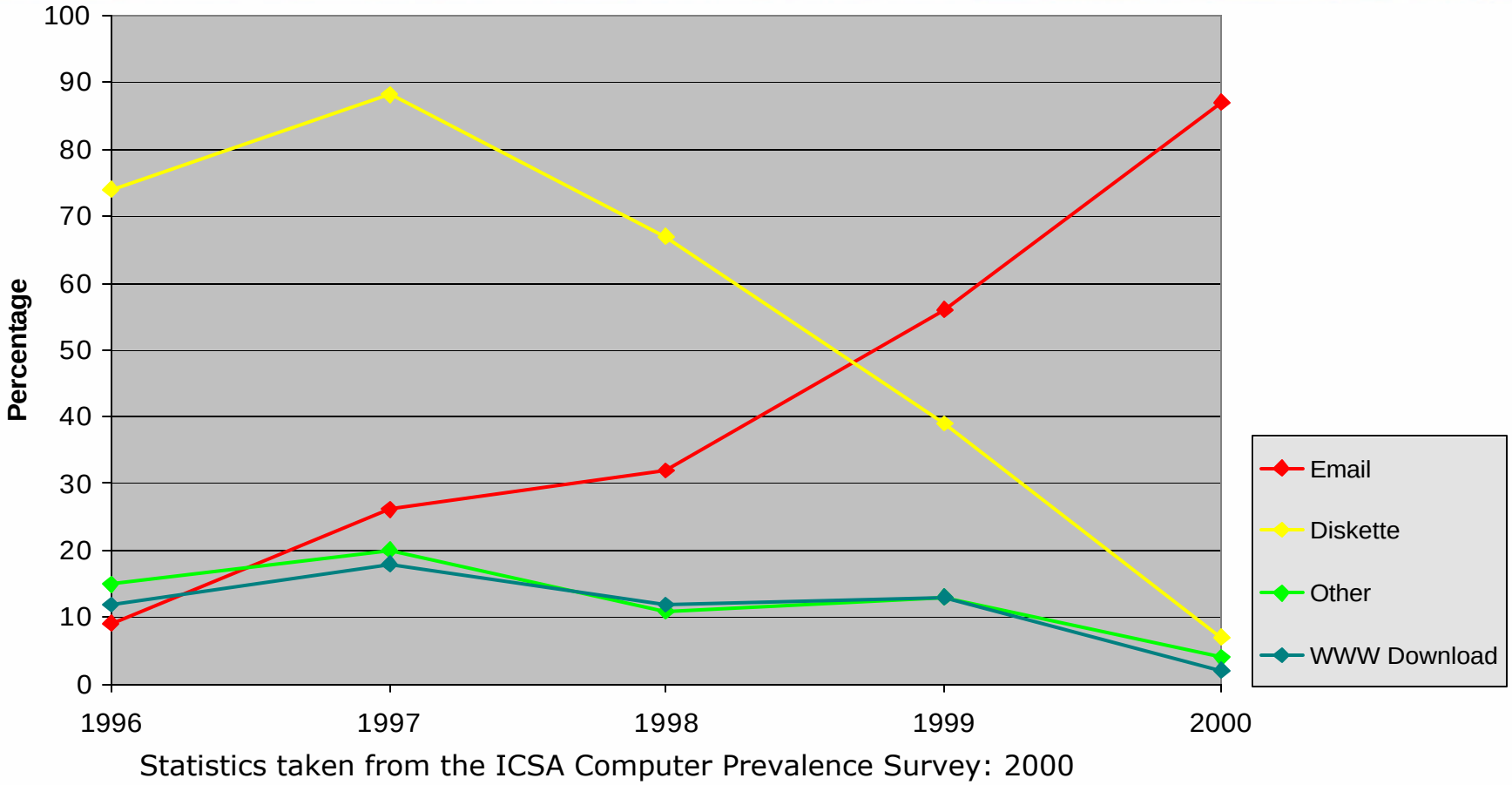
Périmètre de sécurité



Périmètre de sécurité



D'ou proviennent les virus ?



Statistics taken from the ICSA Computer Prevalence Survey: 2000

Antigen
High-Performance Groupware Security

Strategies
Anti-virales:
Microsoft Exchange

Sybari
Ever-Vigilant Protection

Interfaces disponibles

Exchange 5.0/5.5:

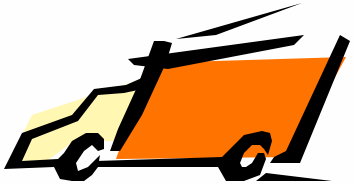
- MAPI – Messaging Application Programming Interface
- AV API – AntiVirus Programming Interface
- ESE API – Extensible Storage Engine Application Program Interface

Exchange 2000:

- VS API – VirusScan Programming Interface
- ESE API – Extensible Storage Engine Application Program Interface

MAPI

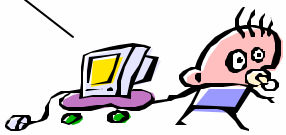
Nouveau message ou accès aux Dossiers Publics



Banque d'Information du serveur Exchange

Alerte MAPI
Notification d'un nouveau message

Protection anti-virus basée MAPI



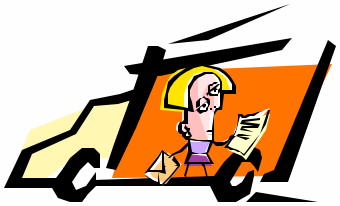
Utilisateur (Client Outlook)

MAPI

- **Connection à toutes les boîtes aux lettres**
  - Protection retardée des boîtes aux lettres
  - Problèmes lors d'actions telles que Deplacer/Ajouter/Supprimer
- **Laisse passer des messages**
- **MAPI n'est pas destiné à une protection anti-virus**
  - Ralentissement des performances
  - Utilisation de CPU accrue
- **Pas de scan des messages "sortants"**
  - Besoin de logiciels supplémentaires

AV API 1.0

Nouveau message ou accès aux Dossiers Publics

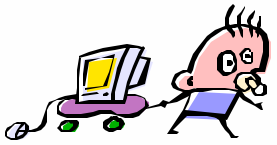


Banque d'Information du serveur Exchange

SP3 Protection Anti-virus dans la Banque d'Information

Utilisateur (Client Outlook)

Protection anti-virus basée MAPI



AV API 1.0: points positifs

- **Accès à la table des attachments**
- **Meilleure performance - intervient au niveau de la Banque d'Information**
- **Chargement et déchargement dynamique du moteur d'analyse (.DLL)**
- **Corrige certaines limitations de MAPI**

Microsoft a distribué AV API à tous les éditeurs AV en Juillet 1999, SP3 de Microsoft est sorti en Septembre 1999.

AV API 1.0: points négatifs

- **Pré-requis: Exchange v5.5, SP4**
- **Pas d'accès aux propriétés des messages:**
  - Emetteur et Destinataire non disponibles
- **Problèmes du scan en temps réel de l'IMS**

  Pas de détection de virus tels que Kak.worm car impossible d'accéder au corps du message
- **Impossibilité de filtrer par Nom de Fichier ou Type de Fichier**
- **Pas de statistiques au travers du moniteur de performance**

VSAPI 2.0

- **Corrige les limitations de MAPI et AVAPI 1.0:**
  - Scan du corps des messages
  - Emetteurs et destinataires visibles...

- **Messages**
  - **SMTP** avec attachements
  - **HTTP** avec ou sans attachements

  sont dorénavant scannés (analyse base .STM)

- **Messages deposés dans le lecteur M: (Installable File System) sont scannés**

VSAPI 2.0

- **Exchange 2000 SP1 nécessaire**

- **Les virus peuvent pénétrer dans la Banque d'Information**
  - Même s'ils sont scannés lorsque l'utilisateur y accéde.

  On distingue 3 types de scan:
  - Scan pro-actif
  - Scan lors de l'accès (On-Access Scanning)
  - Scan en tâche de fond (Background Scanning)

ESE API

- Ne s'appuie ni sur MAPI, ni sur AV API
- Supervise les écritures dans la Banque d'Information du serveur Exchange
- Même approche pour les banques d'information publique et privée
- Accès à la table des attachements
- Scan en mémoire

Antigen
High-Performance Groupware Security

Ce que propose

Antigen for Exchange

Sybari
Ever-Vigilant Protection

Interfaces disponibles

Exchange 5.0/5.5:

- ESE API – Extensible Storage Engine Application Program Interface

Exchange 2000:

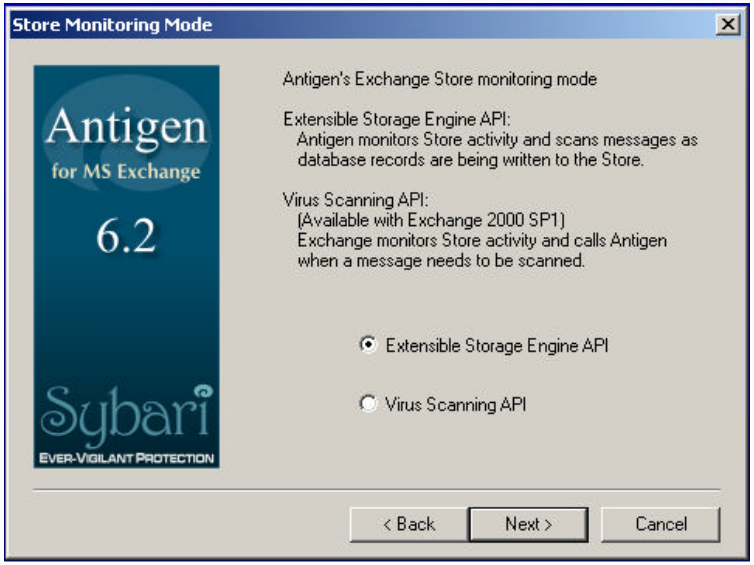
- VS API – VirusScan Programming Interface

OU

- ESE API – Extensible Storage Engine Application Program Interface

Interfaces disponibles

Installation option



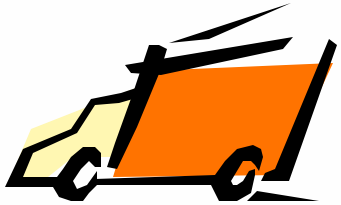
Antutil utility

```
D:\Program Files\Sybari Software\Antigen for Exchange>antutil /mode ese

  ------------------------------------------------------------------------
  Antigen Admin Utility - v6.20.0834
  1998-2001 - Sybari Software, Inc.

     Successfully switched from VSAPI2 mode to classic Antigen shim mode.
```

Antigen for Exchange

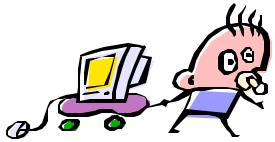
Nouveau message ou accès aux Dossiers Publics

Antigen for Exchange
Protection anti-virus



Banque d'Information du serveur Exchange

Alerte MAPI
Notification d'un nouveau message



Utilisateur (Client Outlook)

Types de scan

	EXCHANGE 5.5	EXCHANGE 2000
Scan Internet	Protection en temps réel de l'ensemble des messages entrants et sortant via l'Internet Mail Connector d'Exchange	Protection du flux SMTP
Scan MTA	Non disponible	Analyse des connecteurs (X400, MS-Mail etc….)
Scan Temps réel	Analyse des "écritures " dans la Banque d'Information d'Exchange	Analyse des GS multiples ainsi que leurs base de données associées. Protection des sauvegardes de fichiers sur le Système de Fichiers Installables (unité M:)
Scan Manuel	Analyse spontanée ou planifiée d'une partie ou de la totalité de la Banque d'Information	Idem

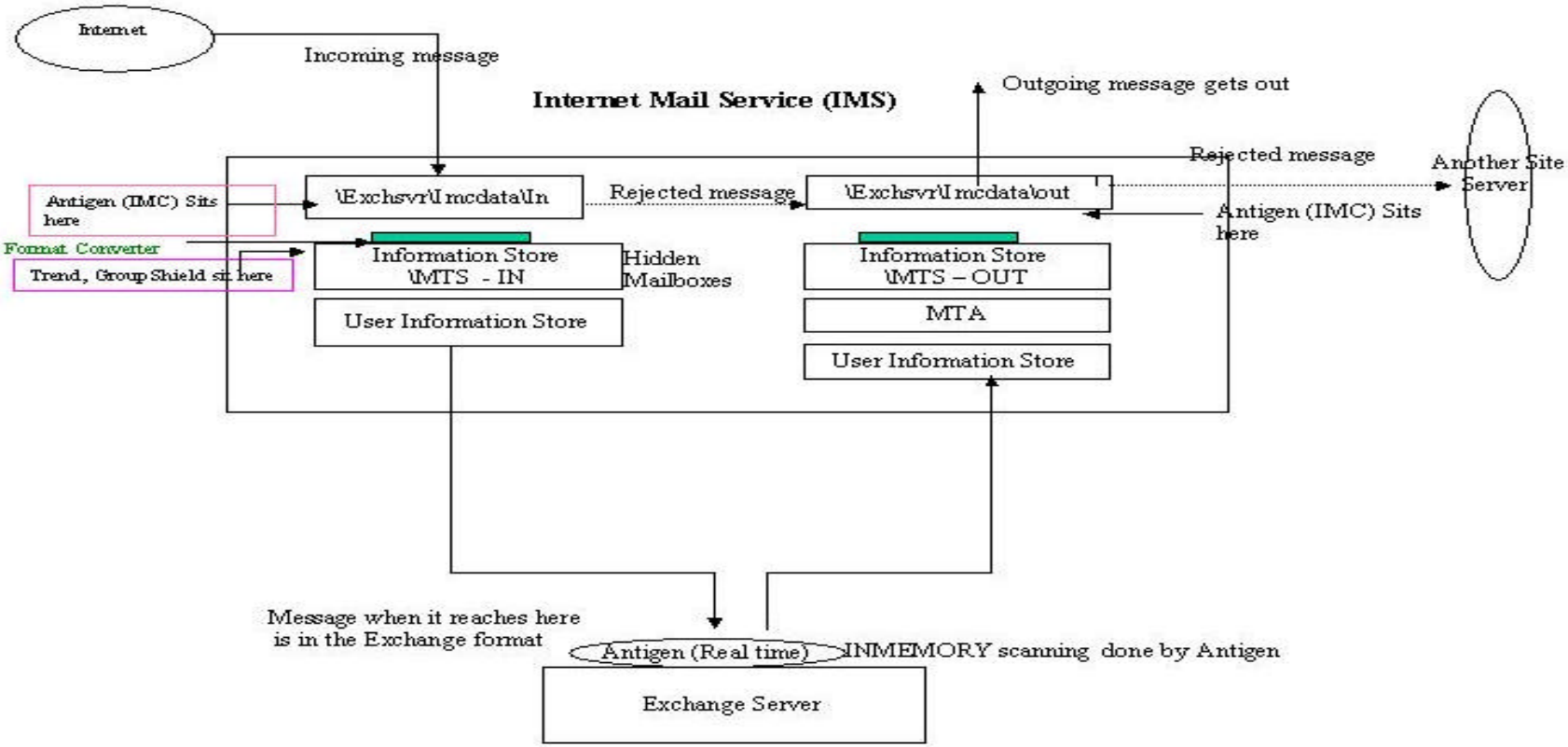
Scan Internet

- **Antigen IMC Process (Exchange 5.5)**

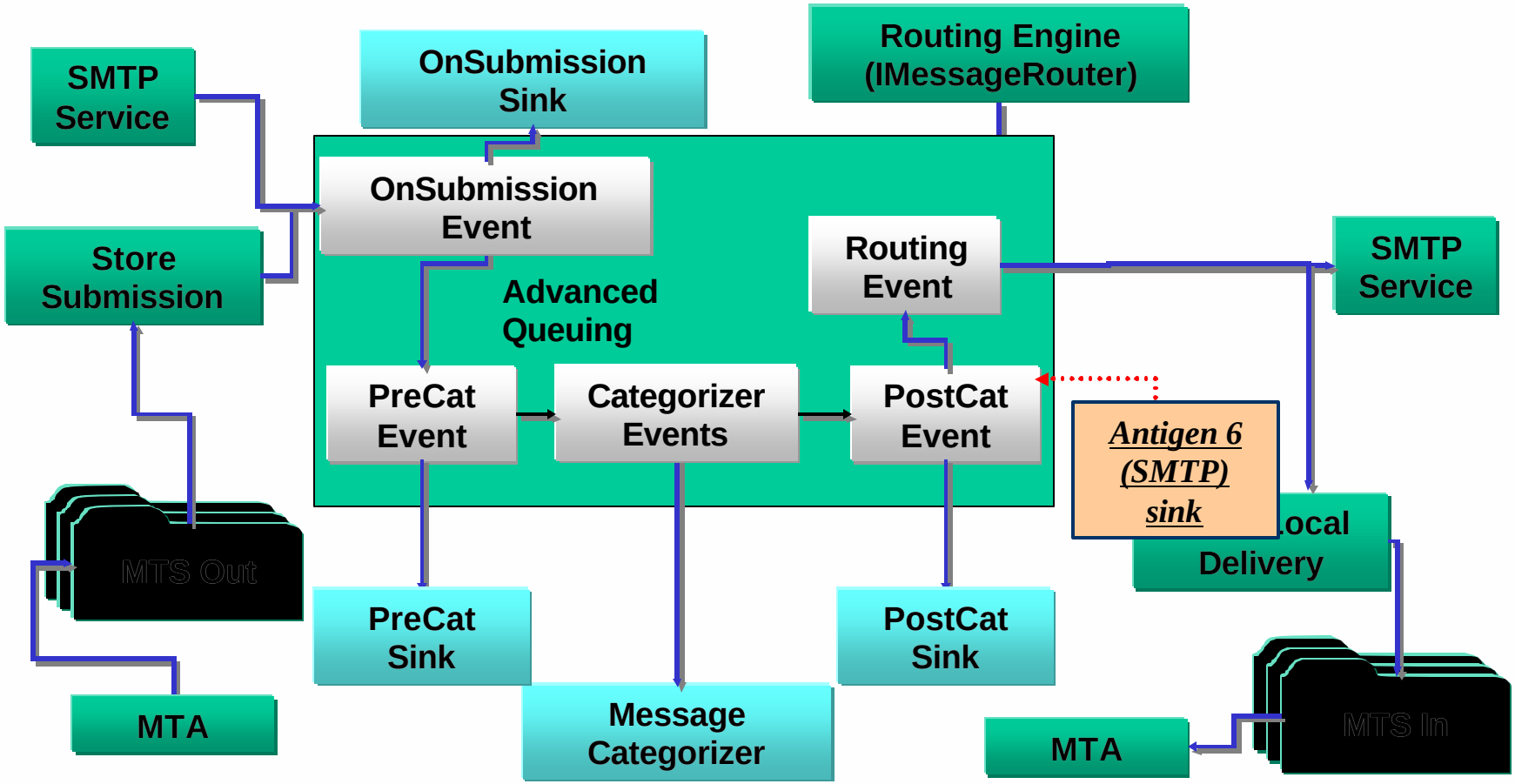
  Protection en temps réel de l'ensemble des messages entrants et sortant via l'Internet Mail Connector d'Exchange

- **Antigen SMTP Process (Exchange 2000)**
  - Protection en temps réel des flux SMTP
  - Utilisation des évènements de transport (SMTP stacks)
  - Protection d'Outlook Web Access
  - Support de plusieurs serveurs Virtuels SMTP
- **100% des messages entrants et sortants sont scannés**
- **Scan en mémoire**

Analyse de l'IMC



Analyse connecteur SMTP



Scan en temps réel

Exchange 5.5:

- **Protection en temps réel de l'ensemble des dossiers publics et des B.A.L des serveurs Exchange.**

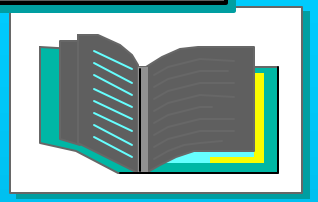
  Analyse des "écritures " dans la Banque d'Information d'Exchange , tous les objects Exchange comportant des pièces jointes sont scannés lors de leur création ou de leur modification

- **Single instance message scanning**
- **Trusted Scanning**
- **Analyse en memoire:**
  - des pièces jointes
  - fichiers à compression ZIP imbriqués

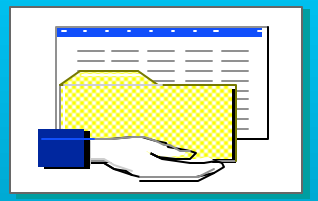
Exchange 5.5: Rappels

Antigen
High-Performance Groupware Security

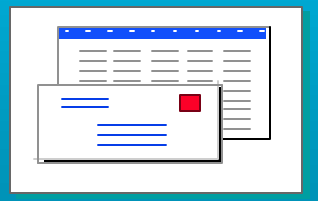
Types de bases



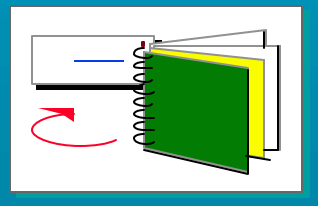
Annuaire



Banque d'Information Publique



Banque d'Information Privée



Synchronisation d'annuaire

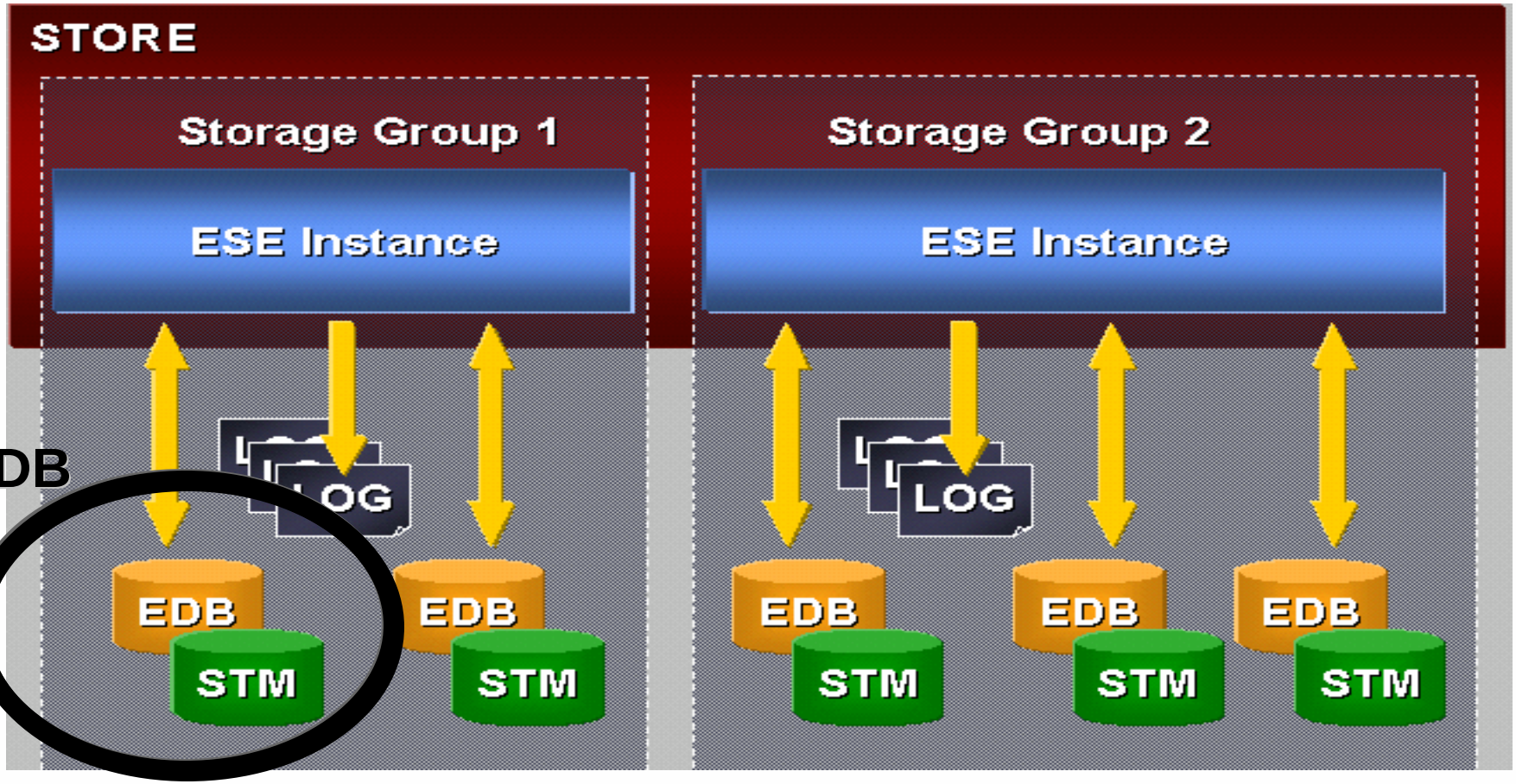
Sybari
Ever-Vigilant Protection

Scan en temps réel

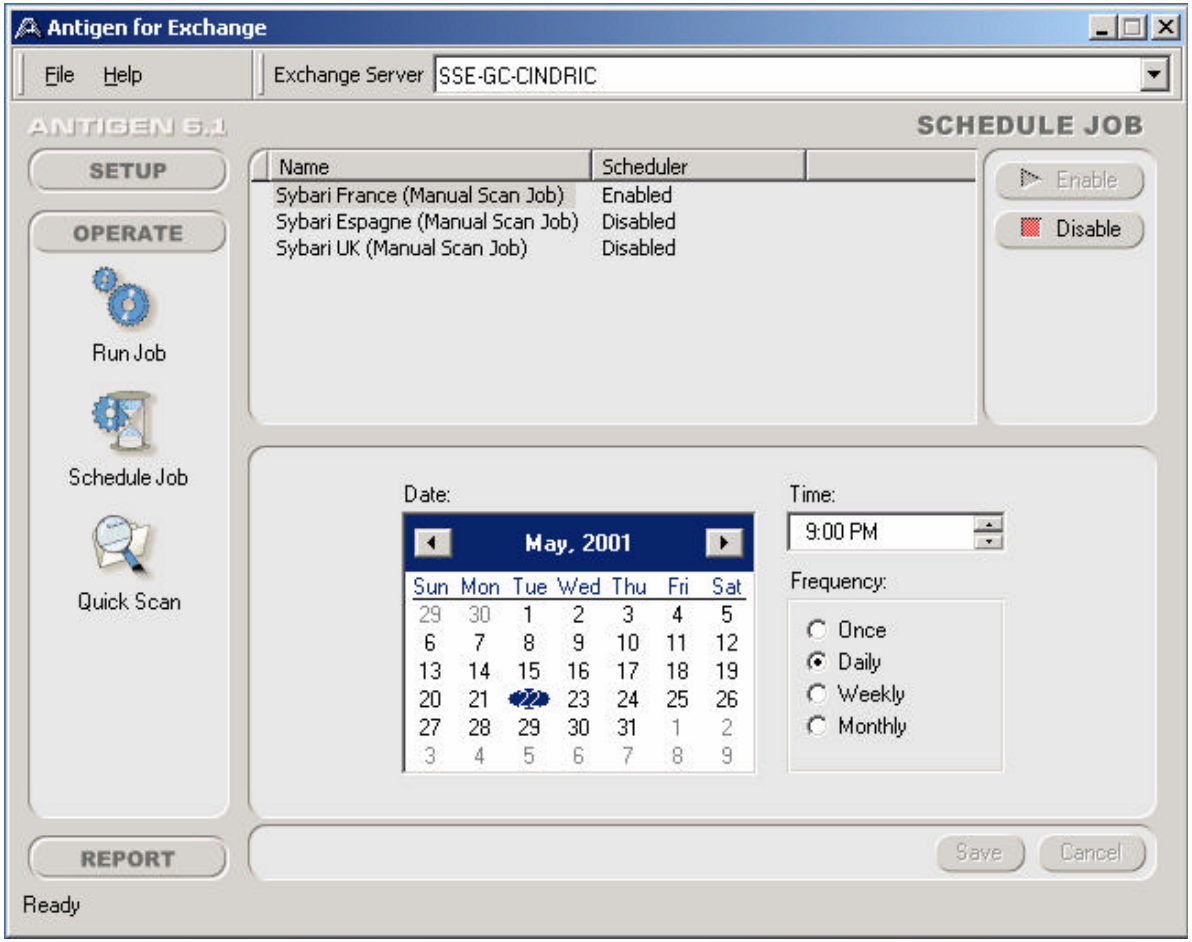
Exchange 2000:

- **Prise en compte des groupes de stockage multiples ainsi que leurs base de données associées.**
- **Protection des sauvegardes de fichiers sur le Système de Fichiers Installables (unité M:)**
- **Protection complète du Systeme de Stockage Web d'Exchange 2000**
- **Single instance message scanning**

Exchange 2000: Rappels

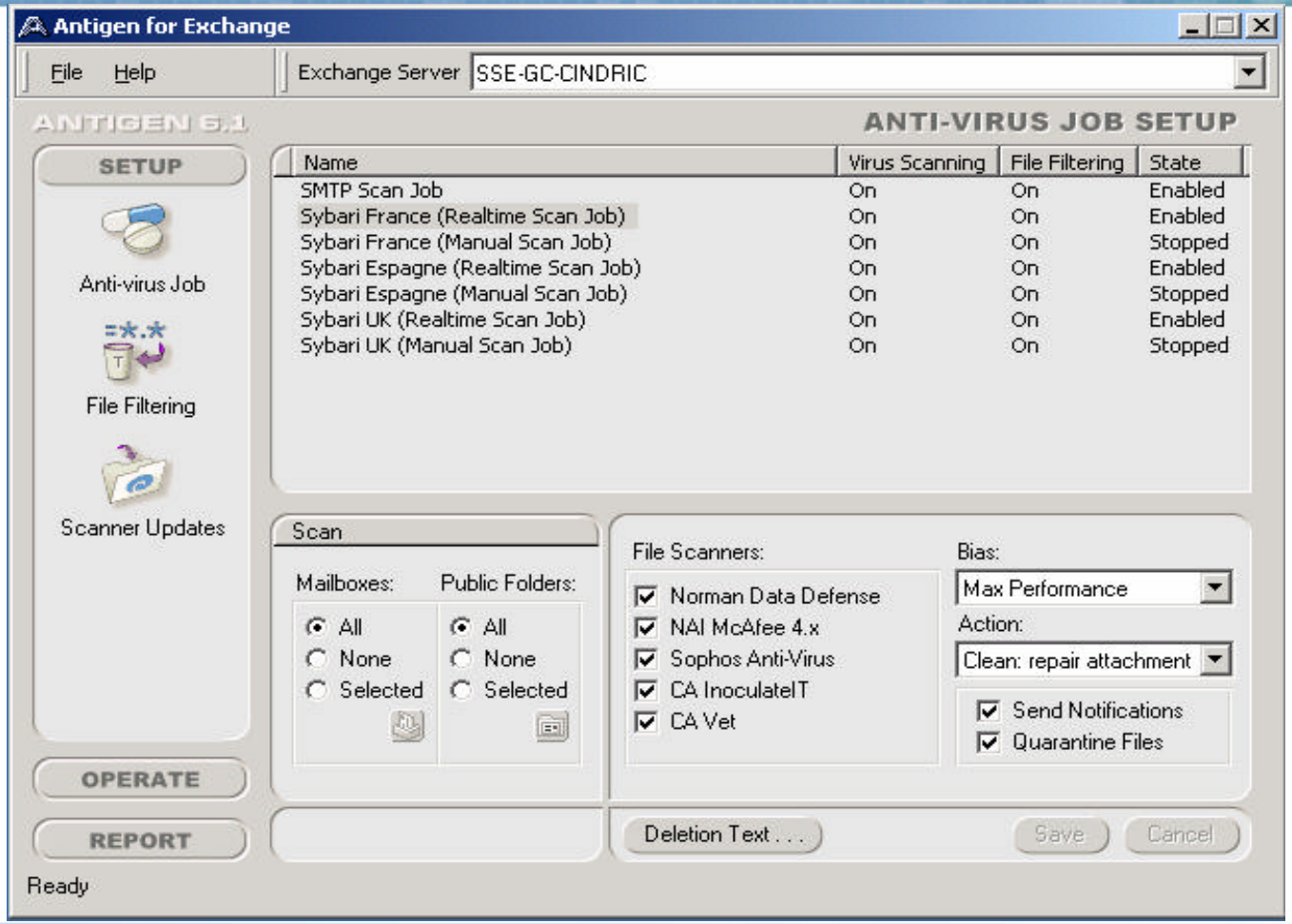


Scan à la demande



Scan à la demande manuel ou planifié de l'ensemble des dossiers publics et des BALs des serveurs Exchange.

Antigen for Exchange



Moteurs d'analyse

Antigen a la faculté d'intégrer jusqu'à 6 moteurs d'analyse: McAfee, Sophos, CA Vet, CA Iris, Norman et Kaspersky

Plusieurs moteurs d'analyse peuvent être utilisés simultanément

Différents moteurs peuvent être assignés à différentes tâches

Exemple :

NAI / Sophos 🕓 Manual Scan
CA / NAI /Norman 🕓 Realtime Scan
Kaspersky / Sophos 🕓 SMTP Scan

Il existe un gestionnaire de moteur qui permet d'assigner divers degrés de priorité qui varient d'un maximum de performance à un maximum de certitude.

Gestionnaire de moteurs

Bias Mode	Description
Max Certainty	Sets the bias setting at 100%. This setting results in all engines being used on every scan in the detection of viruses.
Favor Certainty	Sets the bias setting at 75%. In order to reach the desired certainty level of 75%, Antigen will statistically determine based on the results of the current and previous scans, how many engines will be used during the current scan, which engines, and in which order.
Neutral	Sets the bias setting at 50%. In order to reach the desired certainty level of 50%, Antigen will statistically determine based on the results of the current and previous scans, how many engines will be used during the current scan, which engines, and in which order.
Favor Performance	Sets the bias setting at 25%. In order to reach the desired certainty level of 25%, Antigen will
	statistically determine based on the results of the current and previous scans, how many engines will be used during the current scan, which engines, and in which order.
Max Performance	Sets the bias setting to its lowest value. This setting results in the maximum performance possible when using multiple engines. Antigen will statistically determine based on the results of the current and previous scans, how many engines will be used during the current scan, which engines, and in which order. Antigen is guaranteed to use at least one engine on every scan.

La gestion des moteurs se fait à travers l'option 'Bias'

Option de Purge et Filtrages

Autres options de sécurité:

- **Option de Purge: éliminer tout message infecté par un ver**

- **Filtrages possibles par:**

  - attachements (nom, extension et type)
  - sujet
  - émetteur / nom de domaine

Idéal en cas d'attaques de nouveaux virus avant disponibilité des fichiers de définition de virus

Antigen
High-Performance Groupware Security

Ce que propose

Antigen for Lotus Notes

Sybari
Ever-Vigilant Protection

Composants d'Antigen

Antigen Administrateur

- Administration et configuration d'Antigen

NWall (serveur uniquement)

- Scan en continu des flux de messages entrants et sortants

NShield

- Scan en temps réel des bases de données

NScan

- Scan manuel, planifié ou en ligne de commande

Quarantaine

- Base utilisée pour isoler les virus détectés

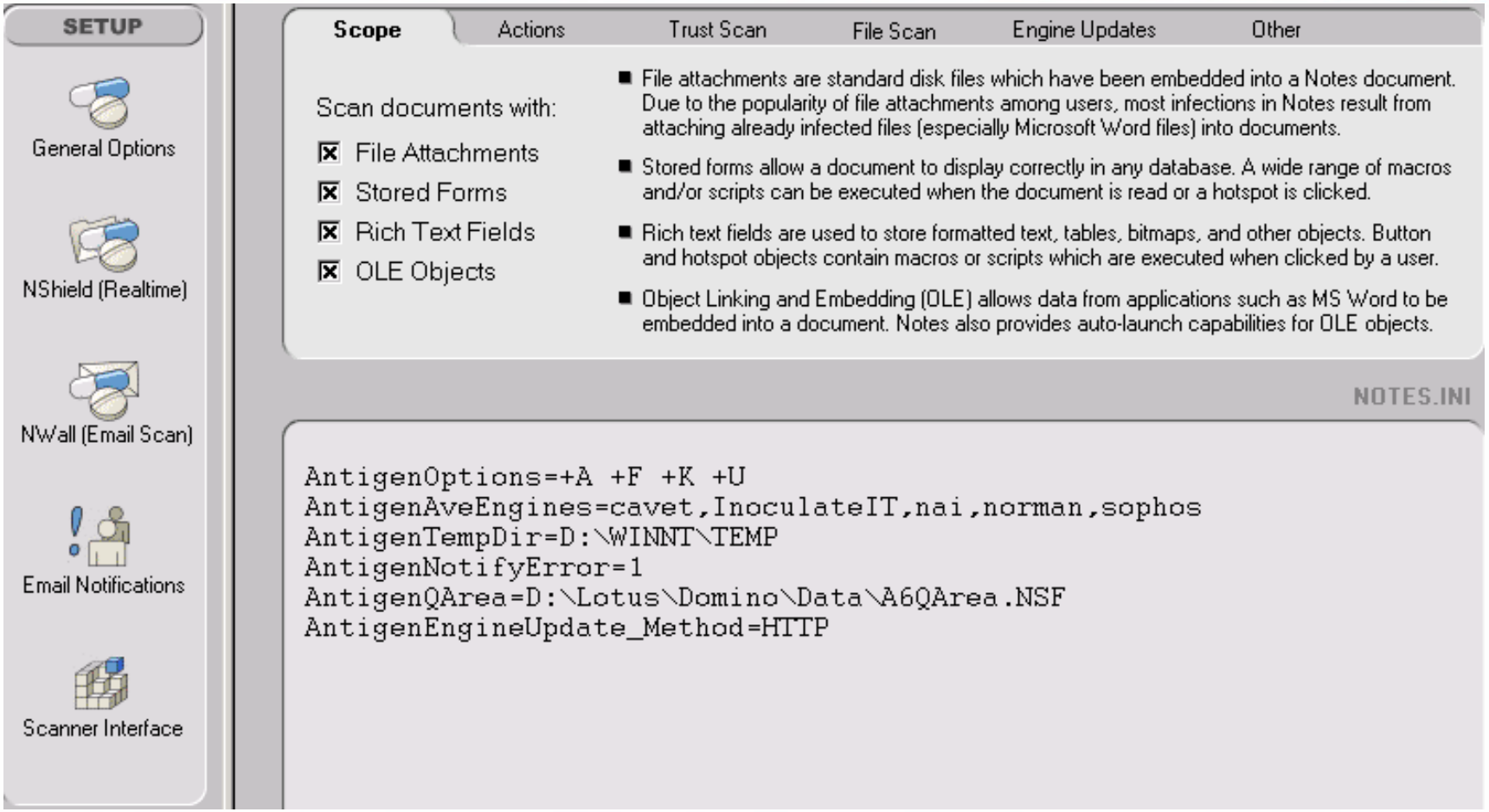
Antigen Administrateur

Base de donnée Notes qui agit comme une interface pour:

- configurer, superviser et faire du troubleshooting sur les composants d'Antigen
- générer des rapports sur les opérations d'Antigen

Utilisation de la technologie LiveNotes pour fournir un mécanisme sûr et dynamique pour manipuler le fichier Notes.ini et d'autres paramètres du système à travers une interface Notes standard.

Antigen Administrateur



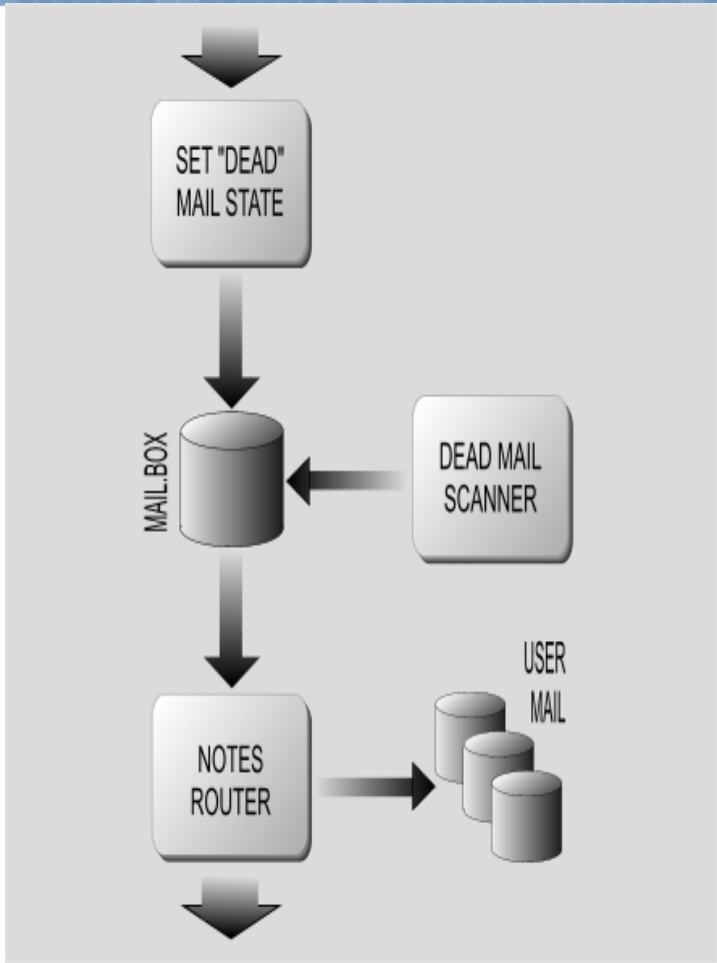
Antigen NWall

Nwall analyse et nettoie en temps réel tous les messages entrants et sortants. Il agit en tant que barrière entre le système de messagerie interne (Notes) et les systèmes de messagerie externes.

Protection du périmètre global des flux de messages:

- Messages SMTP
- Native Notes Client Protection
- iNotes Web access Client
- Native IE & Netscape Mail
- Outlook Client & Outlook Web access Client
- "On-the-fly" Net Store Protection

Approche des concurrents



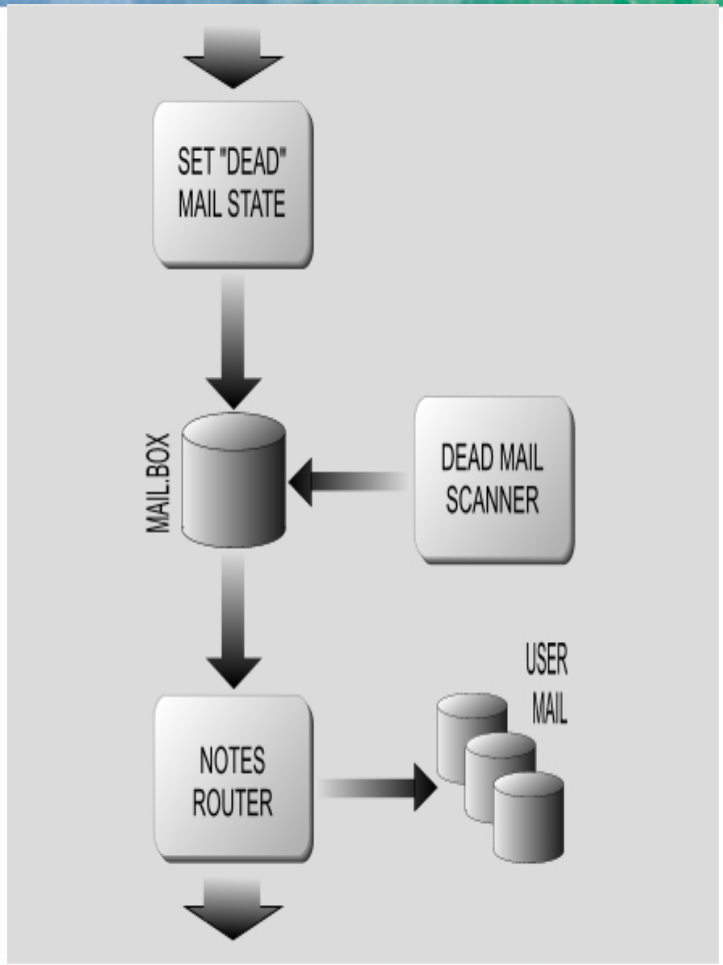
Approche des concurrents

Scan des Messages

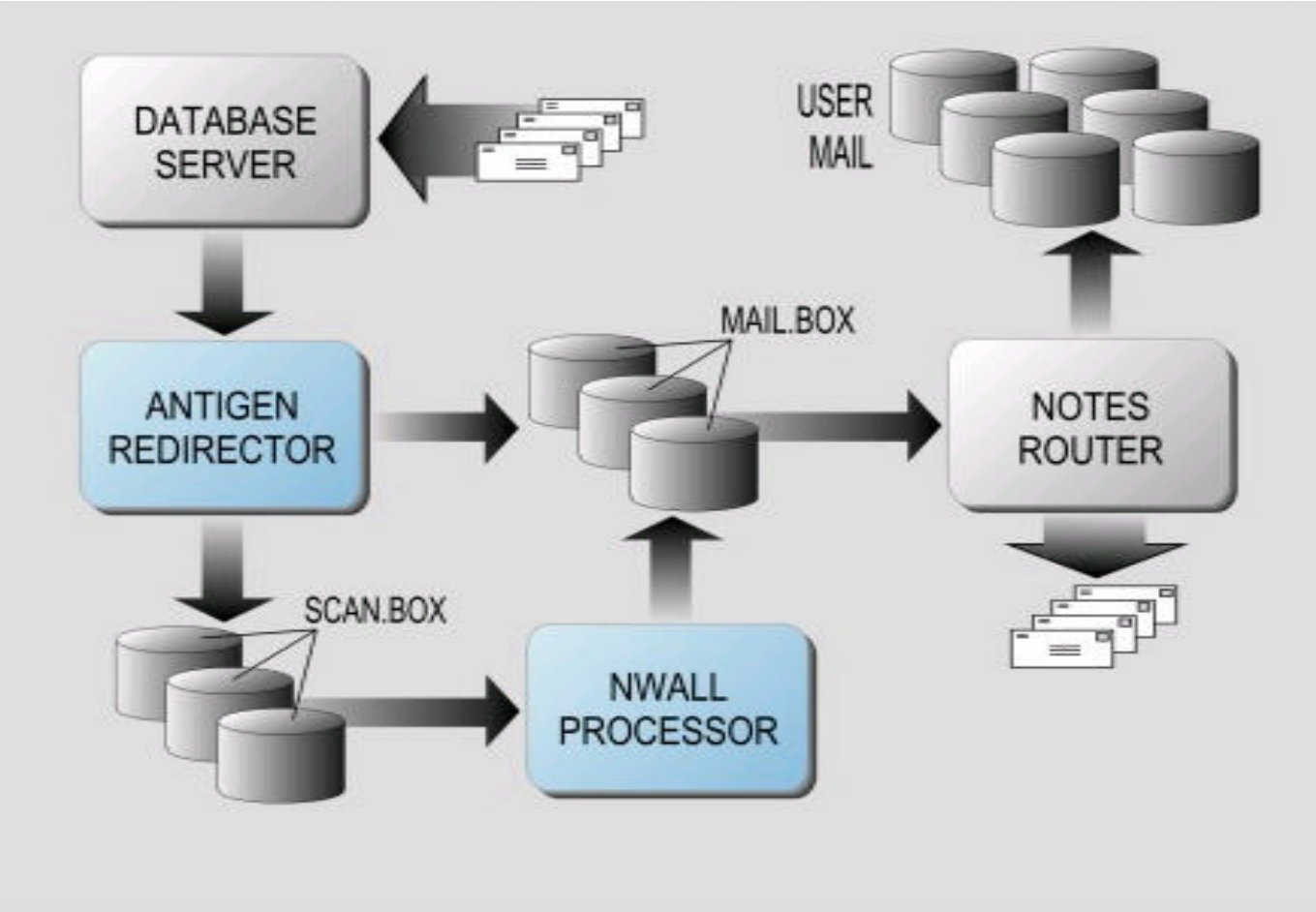
- Supervision de MAIL.BOX

Messages et virus sont écrits dans Mail.box avant analyse

- Conversion nécessaire: passage du message à l'état DEAD (ou HOLD sous R5)
- Interférences avec les Stats
- Interférences avec la supervision du routage des mails (masque les réels problèmes de routage)
- Problème de performance quand charge importante
- Impacte MAIL.BOX et augmente le risque de corruption de MAIL.BOX



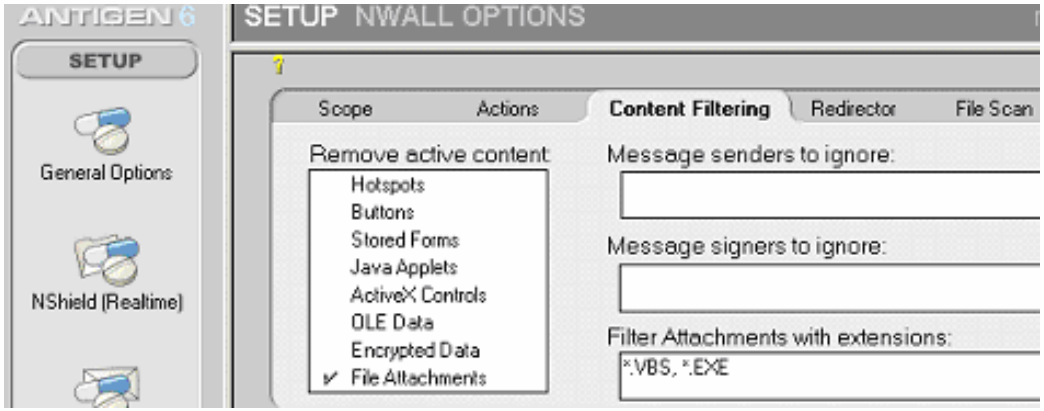
Approche Antigen



Approche des concurrents

Antigen 6.0 supprime les contenus actifs tels que:

Hotspots
Stored Forms
Applets Java
Contrôles ActiveX
Encryption
OLE data



Possibilité d'ajouter des:

- règles de filtrage d'attachements par extensions
- règles d'exceptions par émetteurs et/ou signataires

Antigen NShield

Nshield offre une protection en temps réel des bases Notes et de leurs attachements: lecture et/ou écriture.

-Scan des documents accessibles depuis un browser Web

-Exclusion possible de certaines bases de données du scan

-Ignorer certaines tâches Notes

-Supervise et empêche les attaques du Carnet d'adresses et l'Email Spoofing

-Trust Scanning (élimine les scans redondants)

-Notifications personnalisables

Antigen NScan

Nscan est le module permettant de lancer des scans manuels ou planifiés.

Des scans peuvent être lançés depuis:

- l'interface de l'administrateur Antigen
- une ligne de commande
- à la console du serveur Domino
- le menu Démarrer

Les scans peuvent être planifiés en utilisant le document Programmes défini dans le répertoire Domino.

Scans incrémentaux également disponibles.

Moteurs d'analyse

Antigen a la faculté d'intégrer jusqu'à 6 moteurs d'analyse: McAfee, Sophos, CA Vet, CA Iris, Norman et Kaspersky

Plusieurs moteurs d'analyse peuvent être utilisés simultanément

Différents moteurs peuvent être assignés à différentes tâches

Exemple :

NAI / Sophos 🕓 NScan
CA / NAI /Norman 🕓 NShiels
Kaspersky / Sophos 🕓 NWall

Il existe un gestionnaire de moteur qui permet d'assigner divers degrés de priorité qui varient d'un maximum de performance à un maximum de certitude.

Conclusion

- Nécessité de mettre en place un anti-virus sur les environnements de messagerie
- Filtrage devient de plus en plus nécessaire
- Engendrer un impact minimum sur les serveurs
- Definir une politique anti-virale (procédure à appliquer lors de la sortie d'un nouveau virus, former et éduquer etc…) pour être proactif.

Questions/Réponses