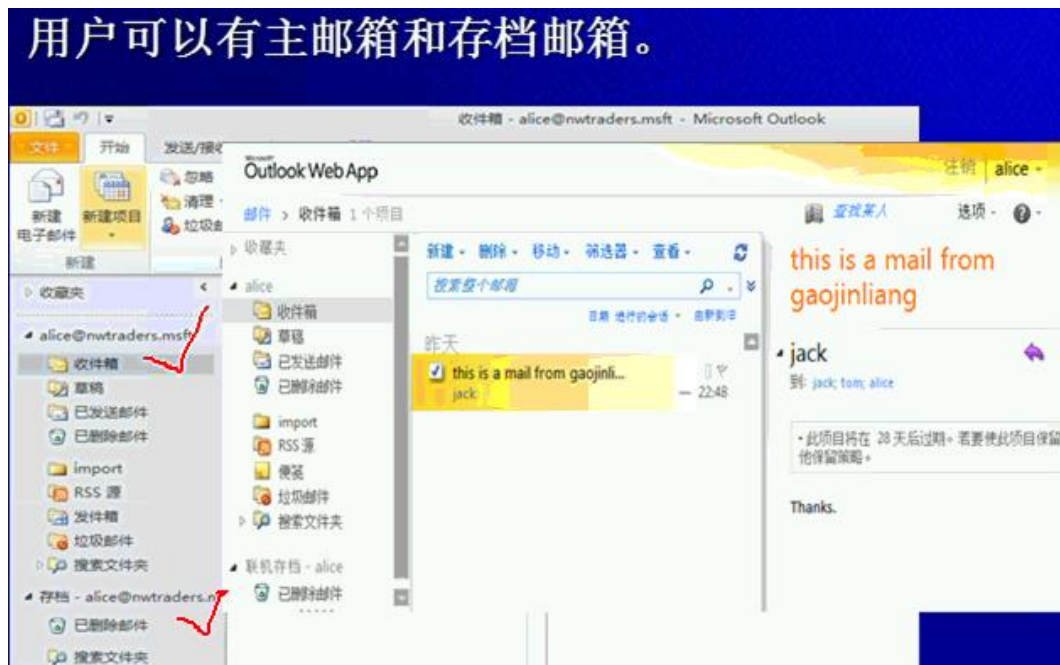


Exchange server 2010信息归档和保留

归档保留和取证两个方面。



个人归档邮箱。



保留策略。

针对某个文件夹或某封邮件实行保留策略。



多邮箱搜索。

◆ 方便合规人员进行多邮箱的搜索



outlook本地归档的缺点，属于非托管的归档方案。

- ◆ Outlook 使用 .pst 文件将数据存储在用户计算机本地或网络共享中。
- ◆ 非托管文件
- ◆ 发现成本增加
- ◆ 无法应用邮件保留策略
- ◆ 数据失窃风险
- ◆ 邮件数据的分段视图

使用exchange服务器进行存档。

- ◆ 主邮箱和存档邮箱可以位于不同的数据库
- ◆ 可以应用“移动到存档”策略
- ◆ 为存档邮箱实施存档配额
- ◆ 为新邮箱启用个人存档
- ◆ 为现有邮箱启用个人存档
- ◆ 连接已断开的个人存档
- ◆ 禁用邮箱的个人存档

多邮箱搜索的作用。

- ◆ 使授权用户能够在整个 **Exchange 2010** 组织中搜索邮箱。
- ◆ 管理多邮箱搜索
 - 将用户添加到“发现管理”角色组
 - 创建发现搜索
 - 开始或停止发现搜索
 - 修改发现搜索
 - 删除发现搜索
 - 创建发现邮箱
 - 使用邮箱搜索删除邮件

如果在ECP中删除多邮箱搜索的记录的话，那么当我们去搜索邮箱里面查看的时候，会发现搜索的记录也被删除了，这个要注意！

创建发现邮箱

- ◆ New-Mailbox SearchResults -Discovery -UserPrincipalName SearchResults@contoso.com
- ◆ Get-Mailbox -Resultsize unlimited -Filter {RecipientTypeDetails -eq "DiscoveryMailbox"}

```
计算机: EX01_Metadatas.msft
[PS] C:\>Add-RoleGroupMember -Identity "Discovery Management" -Member jack
[PS] C:\>New-Mailbox searchresults -Discovery -UserPrincipalName searchresults@contoso.com
```

Name	Alias	ServerName	ProhibitSendQuota
searchresults	searchresults	ex01	50 GB (53,687,091,200 bytes)

```
[PS] C:\>Get-Mailbox -ResultSize unlimited -Filter {RecipientTypeDetails -eq "DiscoveryMailbox"}
```

Name	Alias	ServerName	ProhibitSendQuota
DiscoverySearchMailbox...	DiscoverySearchMa...	ex01	50 GB (53,687,091,200 bytes)
searchresults	searchresults	ex01	50 GB (53,687,091,200 bytes)

```
[PS] C:\>
```

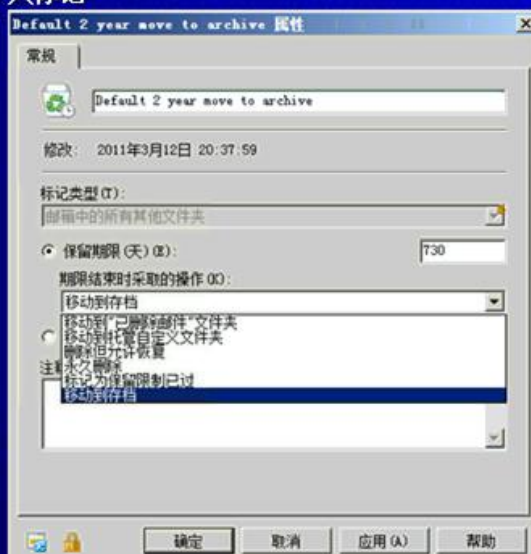
- ◆ 删除发现搜索时，搜索结果也将从发现邮箱中被删除。
- ◆ **SP1**新增功能：
 - 发现管理员可以估计搜索结果以确定发现搜索所返回项目的总数和大小。
 - 可以启用邮箱审核日志记录来审核邮箱所有者、邮箱代理人和邮箱管理员对邮箱的访问权限以及诸如访问和删除文件夹或邮件等的操作
 - 可以启用发现搜索结果的“删除重复”功能，从而仅将特定邮件的一个实例复制到发现邮箱。

邮件记录管理策略 (MRM-P)

- ◆ 保留策略和托管文件夹提供了两种不同的 **MRM** 方法。可以使用任一种 **MRM** 技术在默认文件夹和整个邮箱中强制执行基本 **MRM** 策略。
- ◆ **SP1**的**EMC**下新增保留策略和保留标记的管理，删除了托管文件夹策略的管理。

保留操作。

- ◆ **MoveToArchive**
 - 该操作只能作用于默认策略标记和个人标记
- ◆ **MoveToDeletedItems**
- ◆ **DeleteAndAllowRecovery**
- ◆ **PermanentlyDelete**
- ◆ **MarkAsPastRetentionLimit**



保留策略标记。

三种。

◆ 默认策略标记

- 应用于用户邮箱中所有用户创建的文件夹以及所有电子邮件。此策略不能由用户更改。这是唯一能确保所有电子邮件至少有一个适用策略的策略类型。

◆ 保留策略标记

- 收件箱
- 草稿
- 已发送邮件
- 已删除邮件
- 垃圾邮件
- 发件箱
- **RSS 源**
- 同步问题
- 对话历史记录

◆ 个人标记

- 在保留策略用户界面 (UI) 中显示的策略类型 (UI)，以便用户将其应用于他们创建的文件夹及各个电子邮件。
- 用户不能将这些策略应用于前面所述“保留策略标记”下列出的任何特殊文件夹。
- 用户可以将这些策略应用于特殊文件夹内的电子邮件，但不能应用于文件夹本身。
- 用户可以将这些策略应用于他们自己的用户创建文件夹。

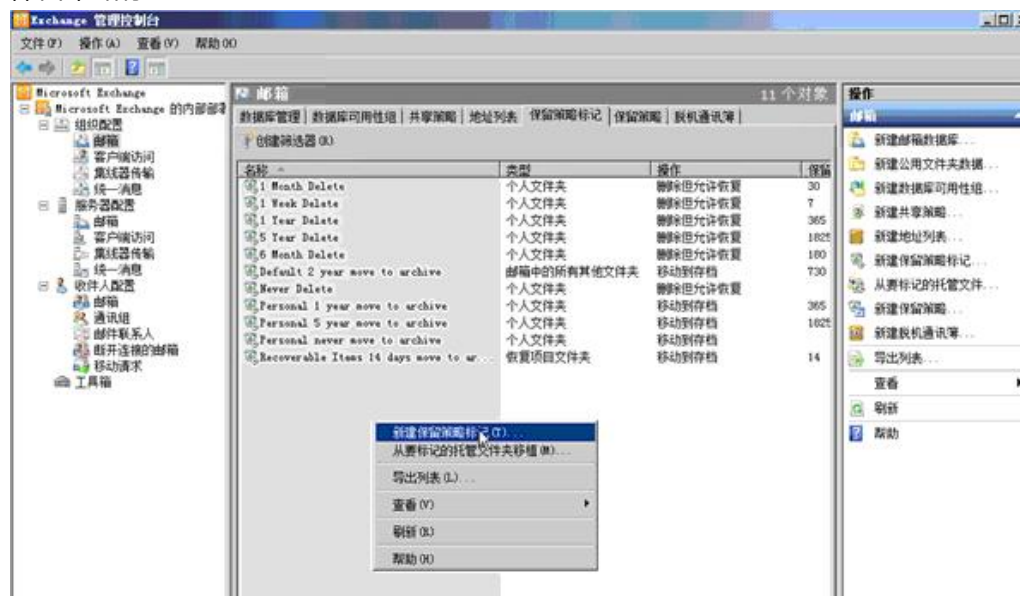
创建保留策略标记——创建保留策略——将保留标记链接到保留策略——应用保留策略——运行托管文件夹助理，默认上午1:00-9:00——处理邮箱。

◆ 手动运行托管文件夹助理。

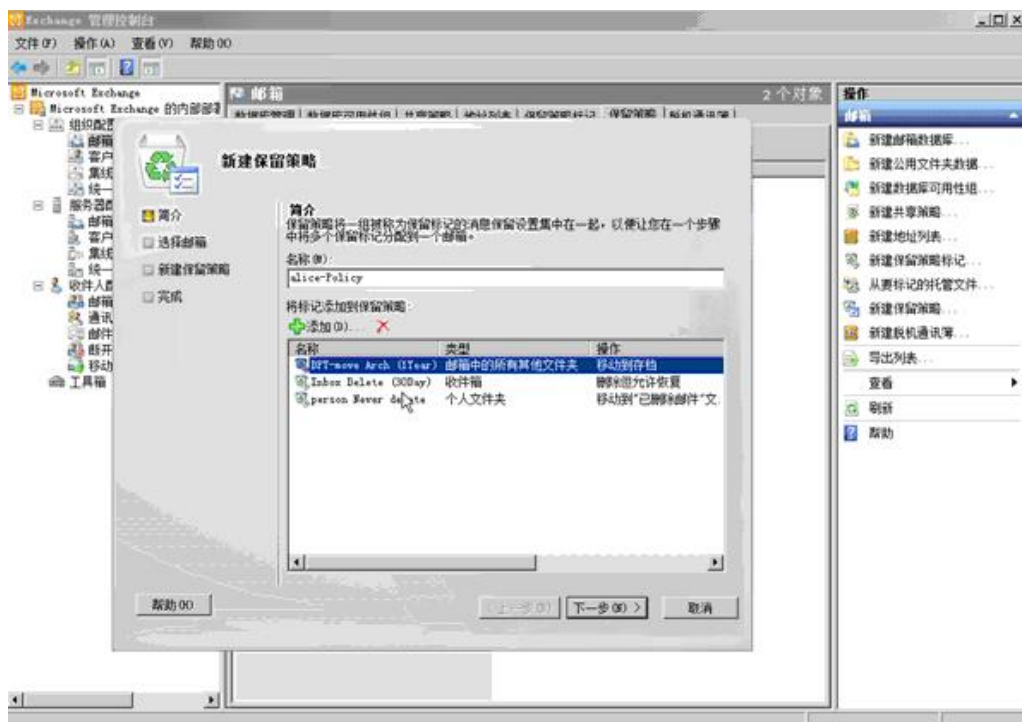
➤ Start-ManagedFolderAssistant -Identity alice



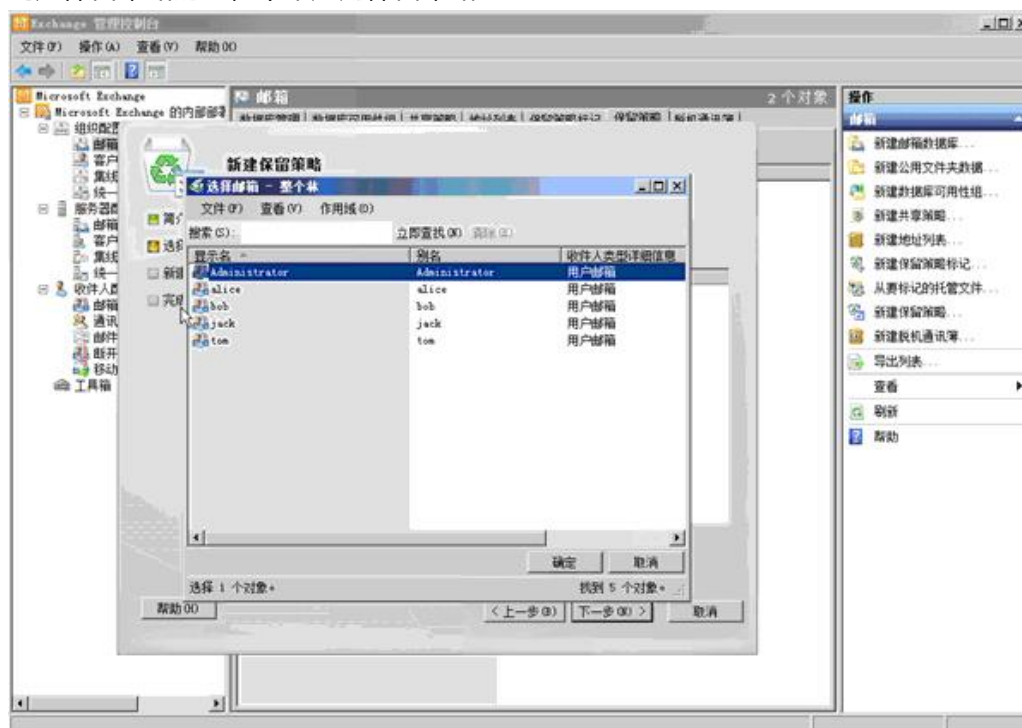
保留策略标记。



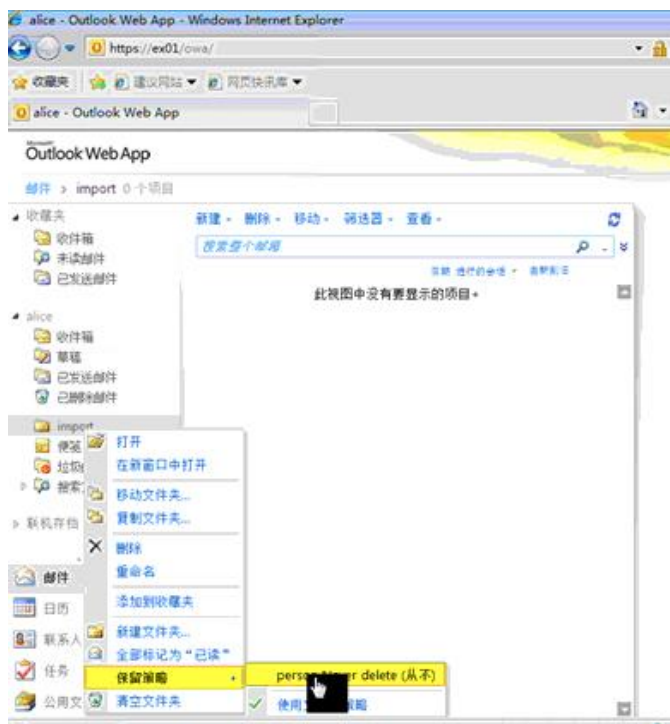
保留策略。



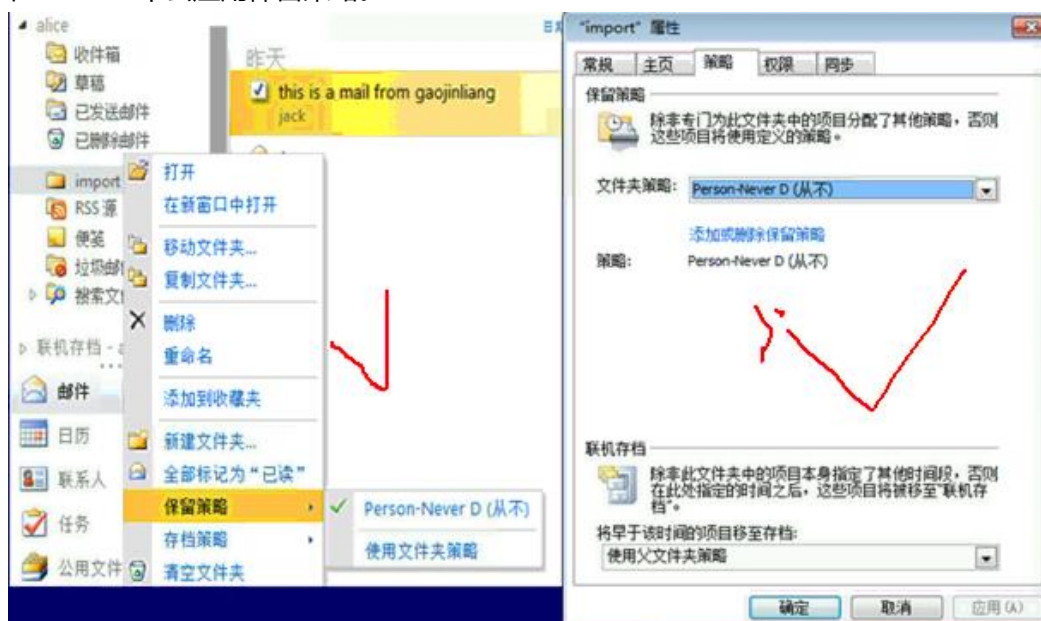
创建保留策略的过程中来应用保留策略。



手动运行托管文件夹助理，让配置马上生效，否则就等到凌晨1:00——9:00。
用户邮箱去选择使用某个保留策略。



在outlook中去应用保留策略。



电子邮件的策略优先顺序

- 针对电子邮件的策略(个人标记)
- 针对包含电子邮件的文件夹的策略
- 针对该文件夹的父级以及父级以上文件夹的策略
- 针对邮箱的策略(默认策略标记)

Exchange Server 2010精讲系列课程(11) Exchange Server 2010安全性-防垃圾邮件及防病毒

exchange server本身并不具备防病毒的功能。


反垃圾功能是借助edge服务器角色。

如果想实现反病毒功能，需要在exchangeserver上面部署反病毒产品，例如forefront protection for exchange或者第三方的产品。




日益增加的安全威胁

- ❖ 垃圾邮件、病毒以及钓鱼网站
- ❖ 网络攻击



日益增加的移动办公需求

- ❖ 需要不受限制的邮件访问
- ❖ 移动办公对于提供企业生产力日趋重要
- ❖ 安全问题变得更加重要



日益增加的法规限制


- ❖ 法规要求趋于复杂化，并且难以强制遵循
- ❖ 担心机密信息的泄露
- ❖ 需要限制对不恰当信息的访问

exchange server 2010的应对策略。




内置的防垃圾邮件功能

- ❖ 利用Edge服务器将垃圾邮件挡在组织之外
- ❖ 多级过滤，提高效率



集成防病毒软件

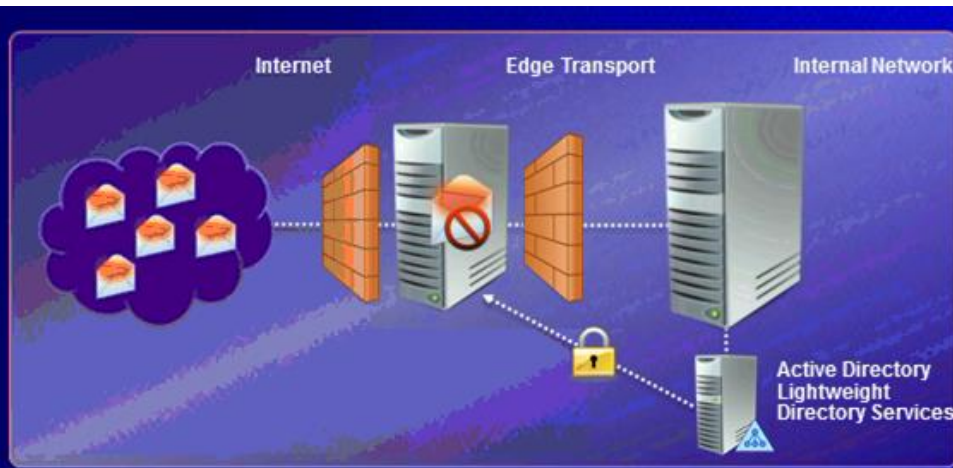
- ❖ 支持on-premise和hosted两种过滤方式
- ❖ 可在线升级的病毒定义



利用加密功能提高邮件安全性

- ❖ 默认情况下所有网络传输都被加密
- ❖ 利用IRM和S/MIME提供对邮件的高级保护

解决方案概述。



Edge服务器角色：

- 部署在DMZ区，与企业内部网络之间有防火墙隔离
- 内置的防垃圾邮件功能，集成的防病毒架构
- 利用safelist以及收件人信息来提供更完善的保护

The screenshot shows the Exchange Management Console (EMC) interface. The 'Edge01' server is selected, and the 'Content Filtering' tab is active. The 'Content Filtering' window shows a list of allowed and blocked content types, including 'anti-spam', 'anti-virus', 'security', 'phishing', 'spam', 'spoofing', and 'virus'.

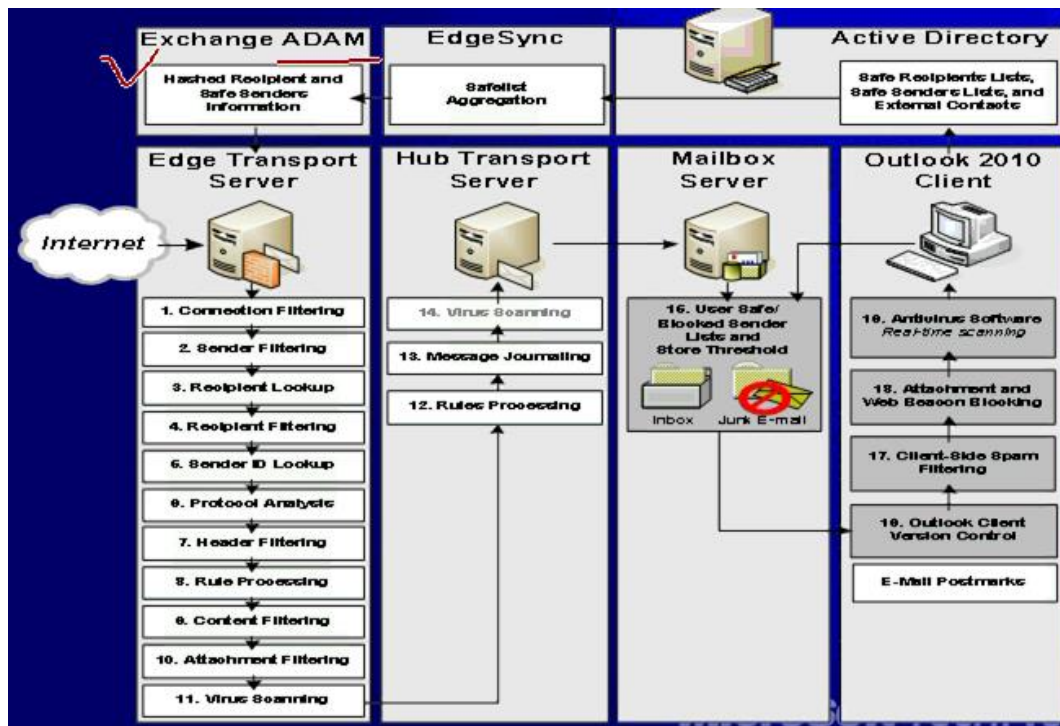
防垃圾邮件代理在Edge上自动安装

这些代理也可以在Hub服务器上安装

防垃圾邮件代理可以利用EMC图形界面轻松管理

多层次的过滤机制。





outlook客户端所做的一些反垃圾操作也会同步到HUB服务器和edge服务器。

Exchange Server 2010邮件防护（传输代理）

- 连接筛选
- 地址重写（入站）
- 边缘规则
- Sender ID
- 收件人筛选
- 发件人筛选
- 内容过滤
- 附件过滤
- 地址重写（出站）

Machine: Edge01 | Scope:

```
(PS) C:\>Get-TransportAgent
```

Identity	Enabled	Priority
Connection Filtering Agent	True	1
Address Rewriting Inbound Agent	True	2
Edge Rule Agent	True	3
Content Filter Agent	True	4
Sender Id Agent	True	5
Sender Filter Agent	True	6
Recipient Filter Agent	True	7
Protocol Analysis Agent	True	8
Attachment Filtering Agent	True	9
Address Rewriting Outbound Agent	True	10

一个典型的SMTP事务

S: 220 foo.com Simple Mail Transfer Service Ready

C: EHLO bar.com

S: 250-foo.com greets bar.com

C: MAIL FROM:Smith@bar.com

S: 250 OK

C: RCPT TO:Jones@foo.com

S: 250 OK

C: RCPT TO:Green@foo.com

S: 550 No such user here

C: RCPT TO:Brown@foo.com

S: 250 OK

C: DATA

S: 354 Start mail input; end with <CRLF>.<CRLF>

C: Subject: This is a test mail.

C: From: abc@123.com

C: To: abc@foo.com

C: Mail body content

C: .

S: 250 OK

C: QUIT

S: 221 foo.com Service closing transmission channel

C: AUTH PLAIN

S: 334

C: AHdlbGRvbgB3M2xkMG4=

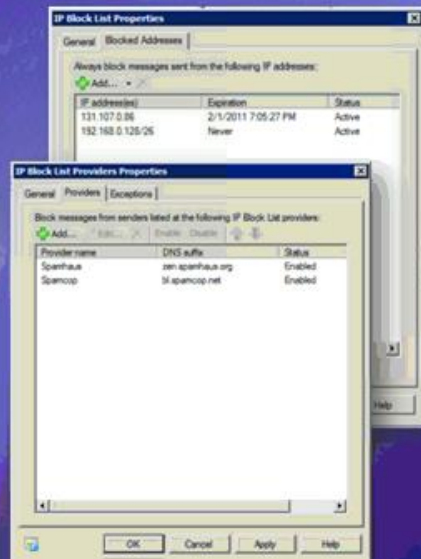
S: 235 2.0.0 OK Authenticated

SMTP 事务	事件触发	防垃圾邮件代理
S: 220 foo.com Simple Mail Transfer Service Ready	OnConnectEvent	Connection Filter Agent
C: EHLO bar.com S: 250-foo.com greets bar.com	OnHeloCommand OnEhloCommand	
C: AUTH PLAIN S: 334 C: AHdlbGRvbgB3M2xkMG4= S: 235 2.0.0 OK Authenticated	OnAuthCommand OnEndofAuthentication	
C: MAIL FROM:Smith@bar.com S: 250 OK	OnMailCommand	Connection Filter Agent Sender Filter Agent
C: RCPT TO:Jones@foo.com S: 250 OK	OnRcptCommand	Connection Filter Agent Recipient Filter Agent
C: DATA S: 354 Start mail input; end with <CRLF>.<CRLF>	OnDataCommand	
C: Subject: This is a test mail. C: From: abc@123.com C: To: abc@foo.com	OnEndofHeaders	Connection Filter Agent/Sender ID Agent/Sender Filter Agent/Protocol Analysis Agent
C: Mail body content C: . S: 250 OK	OnEndofData	Edge Rule Agent/Content Filter Agent/Protocol Analysis Agent
	OnReject	Protocol Analysis Agent
	OnResetCommand	Protocol Analysis Agent
C: QUIT S: 221 foo.com Service closing transmission channel	OnDisconnectEvent	Protocol Analysis Agent

如果IP在RBL里面，则被拒绝掉。

连接筛选

- 检查发起连接的远程服务器
- 利用管理员定义的IP阻止/允许列表
- 支持第3方阻止列表提供程序 (RBL)
 - 外部RBL提供程序会维护一个数据库，其中包含已知的垃圾邮件服务器及IP地址
 - 多数RBL是免费的



发件人



收件人

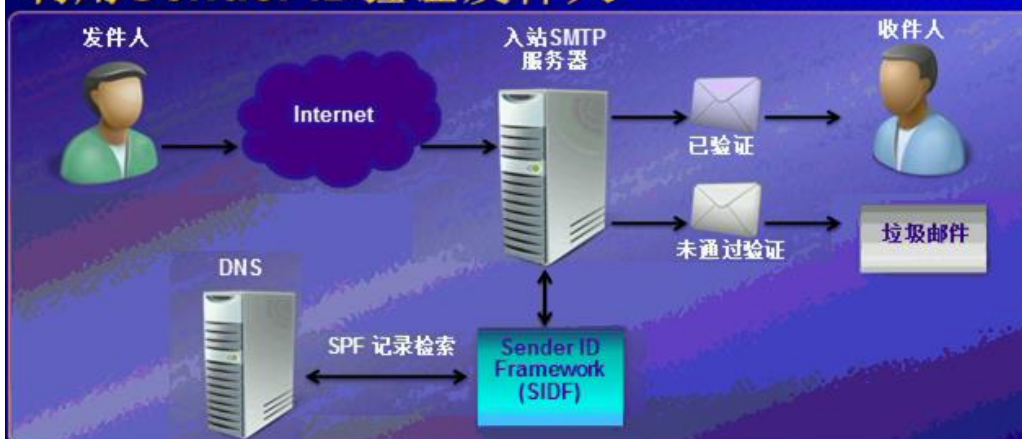
发件人筛选

- 根据发件人地址或域名进行筛选

收件人筛选

- 屏蔽收件人为空，或者在组织中不存在该收件人的邮件
- 管理员定义的阻止列表
- 与收件人词典的集成
- 防止目录搜集攻击 (Directory Harvest Attack)

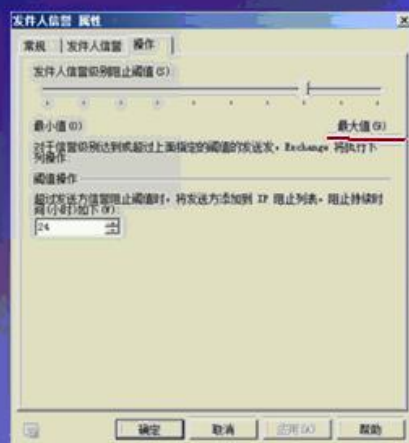
收件人筛选/发件人筛选 利用Sender ID验证发件人



Sender ID 代理：

- 利用Sender ID Framework (SIDF) 验证发件人
- SIDF 在全球已有12M个域参与
- 定位并防范邮件诈骗

发件人信誉值通过windows update进行自动判断。最大值9，垃圾邮件可能性越高。
发件人信誉值无需手动修改，只要服务器开启了windows update，会自行设定。



发件人信誉

- 通过内部分分析和测试来确认发件人信誉
- 为每个发件人创建配置文件，并以此计算发件人信誉等级Sender Reputation Level (SRL)
- 发件人的SRL超过警戒线将被临时屏蔽



过滤的基准：

- ◆ 管理员定义的关键字
- ◆ 基于对数亿封Hotmail邮件分析而演化出的SmartScreen技术

为邮件定义SCL值

- ◆ Spam Confidence Level (SCL)

支持预定义操作

- ◆ 隔离区
- ◆ 用户的垃圾邮件文件夹

随时更新

- ◆ 每两周定时、不定时更新

SCL为9的可能是垃圾邮件。

SCL为0的邮件不可能是垃圾邮件。

SCL即垃圾邮件可信度。

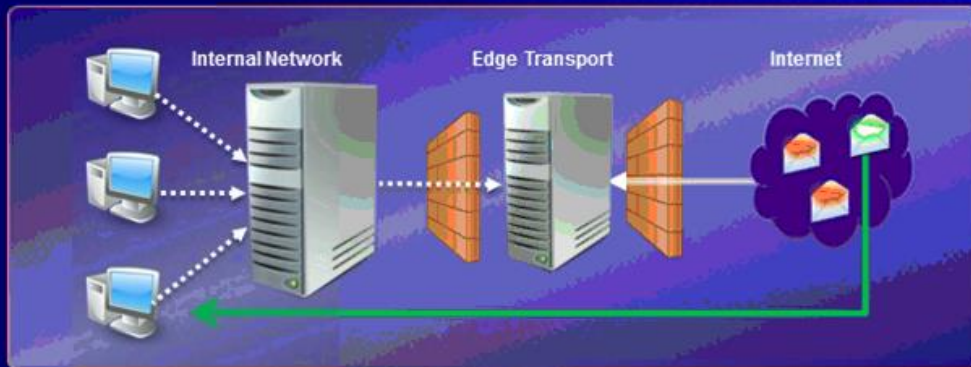
SCL基于smartscreen技术来判断和分析，smartscreen技术来自于Hotmail。

在Edge上实现精准过滤

1. 随时从客户端收集发件人信息

2. 信任列表被同步给Edge服务器

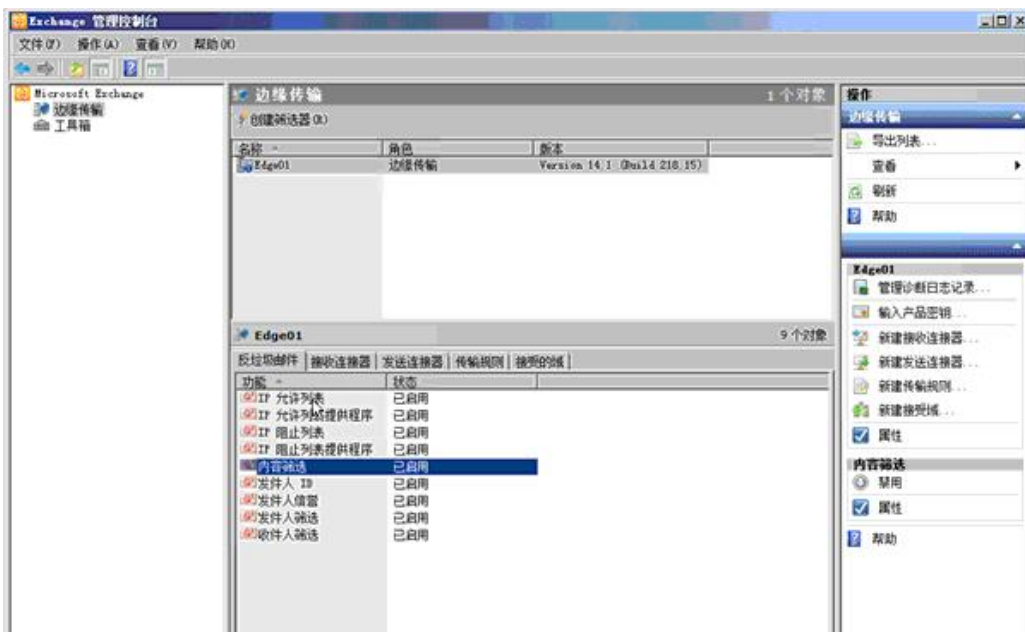
3. 受信任的电子邮件可以绕过内容筛选



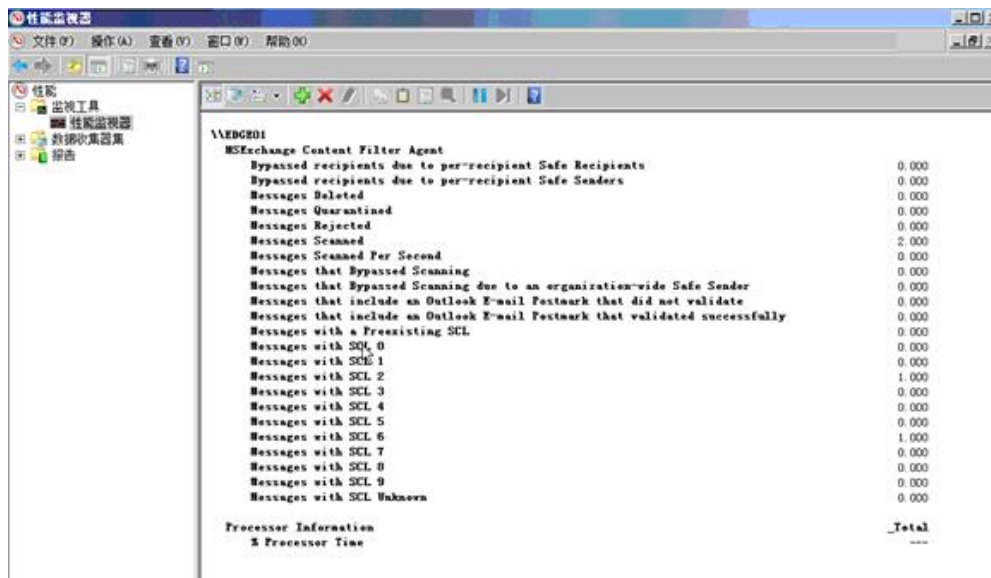
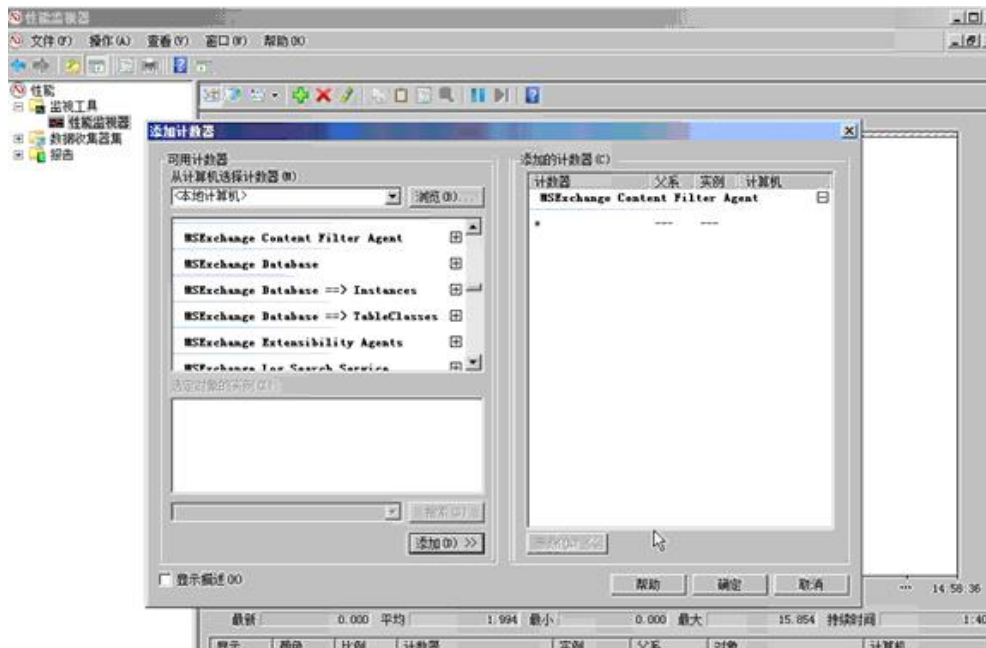
4. 更加智能的筛选功能可以提高效率

前四种是连接筛选。

后四种是收件人或发件人筛选。



性能计数器里面可以打开SCL的性能计数器，可以统计一段时间内的SCL的大小信息。

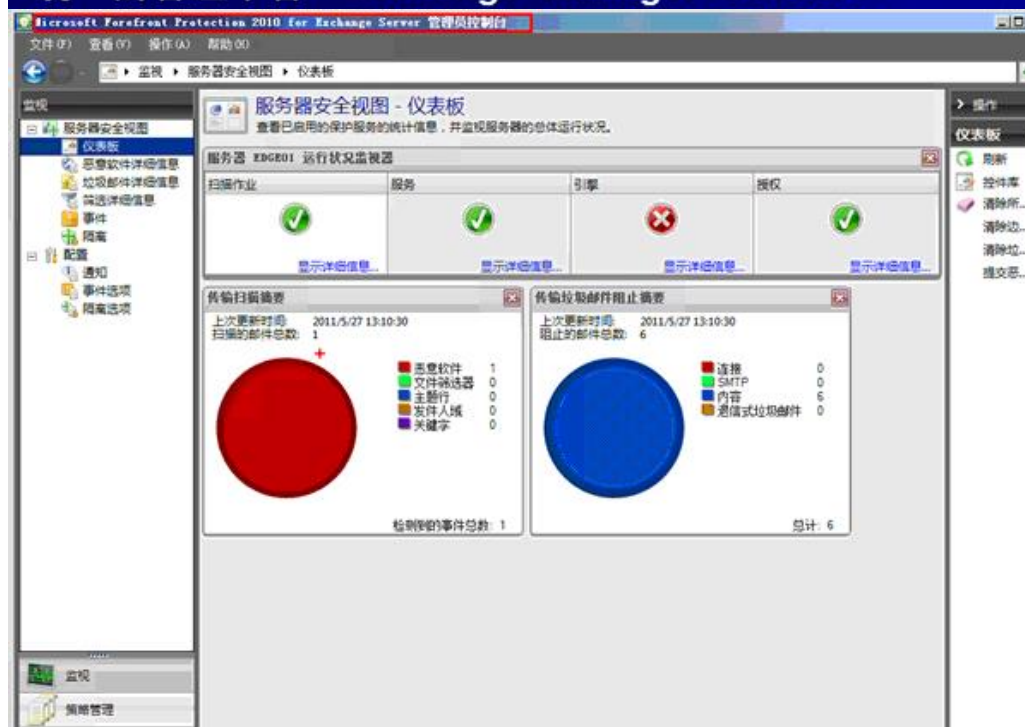
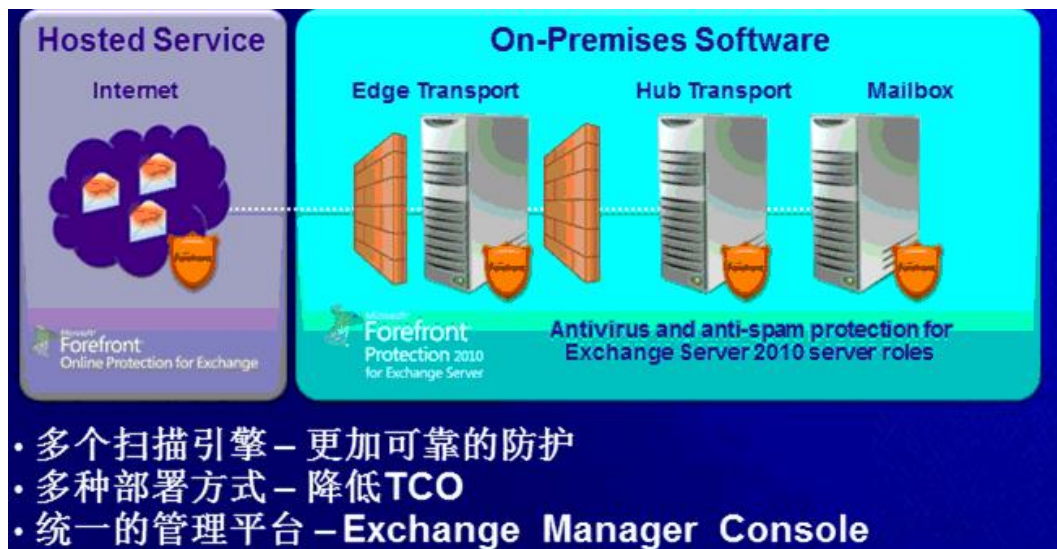


对防病毒的支持。

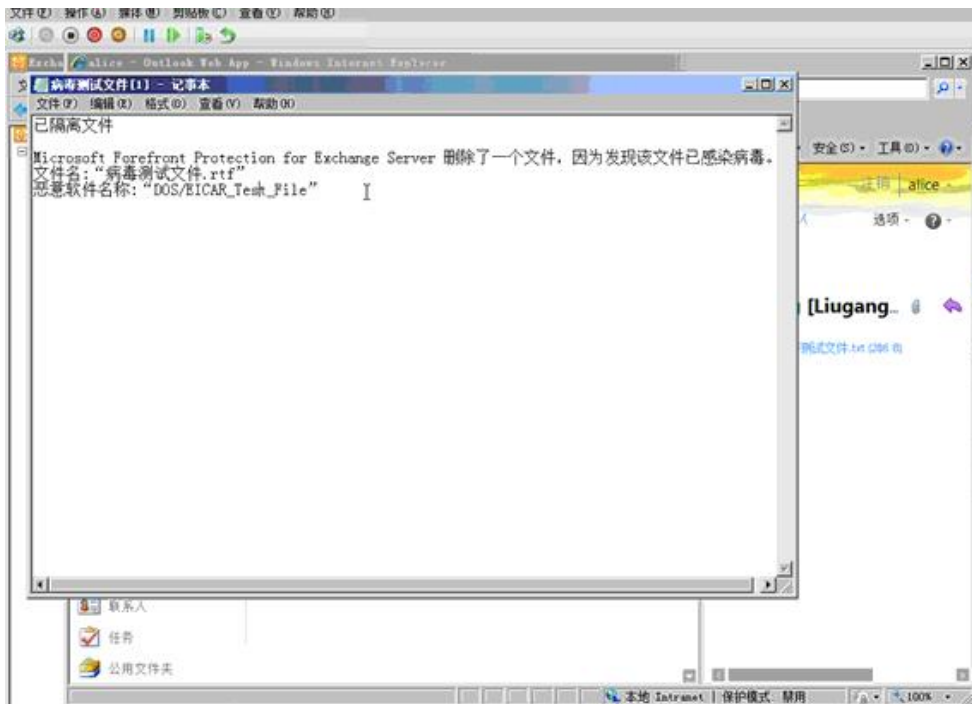
对于邮件标记，要求exchange角色的版本一致。



与FPE的集成。



文件隔离。



Exchange Server 2010 安全性总结



所有网络连接的自动加密



内置的、不断更新的、多层级的垃圾邮件过滤功能



与防病毒软件的轻松集成

=====

Exchange Server 2010精讲系列课程(12)_Exchange Server 2003_7升级到Exchange Server 2010



TNWebCast20110... F.pdf
2.88MB

=====

