

Giáo trình bài tập:**Quản trị bảo mật thư điện tử trong Microsoft Exchange Server 2007****Mục Lục**

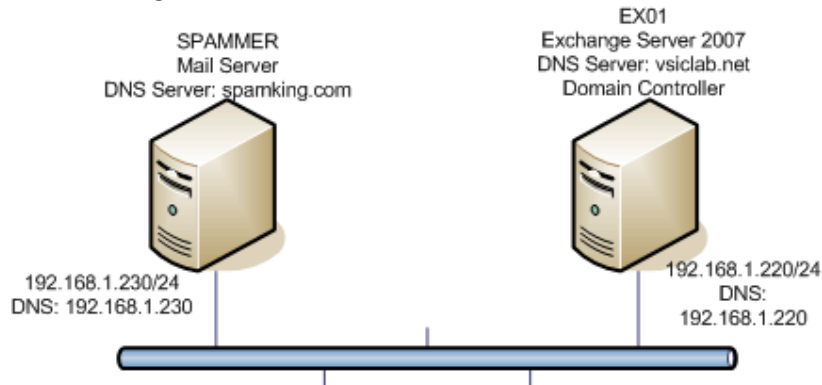
Module 1 Maintaining Antivirus and Anti-Spam Systems	2
Bài tập 1 Sử dụng các tính năng Anti-Spam	2
Chuẩn bị.....	2
Cài đặt Anti-spam Agent cho Hub Transport server	2
Cấu hình Connection Filtering với IP Block List.....	3
Cấu hình Connection Filtering với IP Block List Providers	5
Cấu hình Sender Filtering.....	9
Cấu hình Recipient Filtering	10
Cấu hình Sender ID	11
Cấu hình Content Filtering	15
Bài tập 2 Sử dụng các tính năng Anti-Virus.....	18
Cấu hình Attachment Filtering	18
Module 2 Configuring Edge Transport Servers	20
Bài tập 1 Hiện thực Edge Transport Server Role	20
Sử dụng Security Configuration Wizard để bảo vệ Edge Transport server	20
Cấu hình EdgeSync	29
Bài tập 2 Cấu hình Domain Security	33
Module 3 Implementing Messaging Policies	42
Bài tập 1 Cấu hình Messaging Records Management.....	42
Bài tập 2 Cấu hình luật Transport and Journaling	48

Module 1 Maintaining Antivirus and Anti-Spam Systems

Bài tập 1 Sử dụng các tính năng Anti-Spam

Chuẩn bị

- Thiết lập mô hình mạng như sau:



- Cấu hình Condition Forwarder cho DNS

Trên EX01, forward domain spamking.com sang 192.168.1.230 và trên SPAMMER forward domain vsiclab.net sang 192.168.1.220.

Tạo các MX record cho 2 domain trên 2 DNS Server.

- Cài đặt SMTP Service và POP3 Service trên SPAMMER.

- Cấu hình SMTP Service domain là spamking.com và cấu hình chứng thực là **Basic Authentication**.

- Cấu hình POP3 Service.

Tạo domain spamking.com

Tạo mailbox voldermort trong domain spamking.com

Cài đặt Anti-spam Agent cho Hub Transport server

- Dùng lệnh **install-AntispamAgents.ps1** để cài đặt **Anti-spam Agent**

Vào **Exchange Management Shell**, chuyển vào thư mục **C:\Program Files\Microsoft\ExchangeServer\Scripts** rồi dùng lệnh **install-AntispamAgents.ps1** để cài đặt Anti-spam Agent.

```
Machine: ex01 | Scope: vsiclab.net
[PS] C:\>
[PS] C:\>cd 'C:\Program Files\Microsoft\Exchange Server\Scripts'
[PS] C:\Program Files\Microsoft\Exchange Server\Scripts>.\install-AntispamAgents.ps1
```

Identity	Enabled	Priority
Connection Filtering 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

```
WARNING: The agents listed above have been installed. Please restart Microsoft Exchange Transport service for changes to take effect.

[PS] C:\Program Files\Microsoft\Exchange Server\Scripts>
```

Cấu hình Connection Filtering với IP Block List

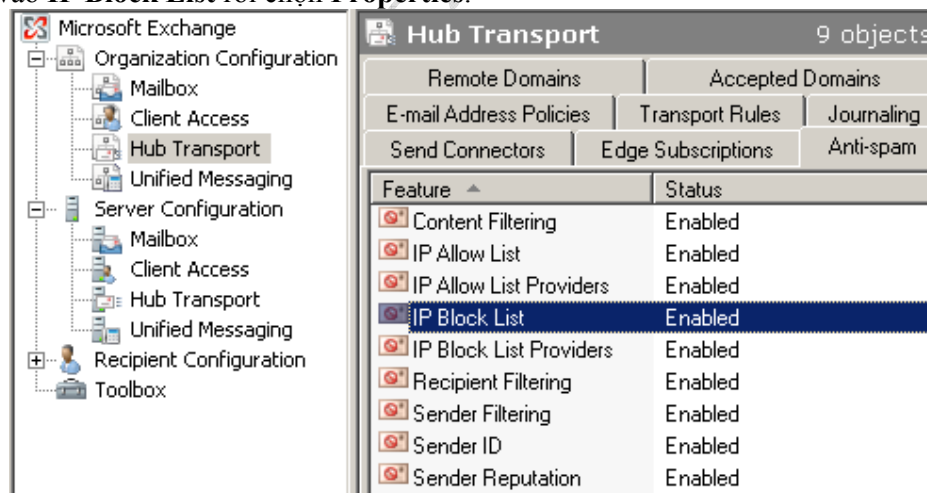
1. Gửi một message từ Voldermort đến Harry. Xác nhận Harry đã nhận được message từ Voldermort

Trên SPAMMER, đăng nhập vào Outlook Express với tài khoản Voldermort, gửi một message đến harry@vsiclab.net với tiêu đề **Test IP Block List – Before config**.

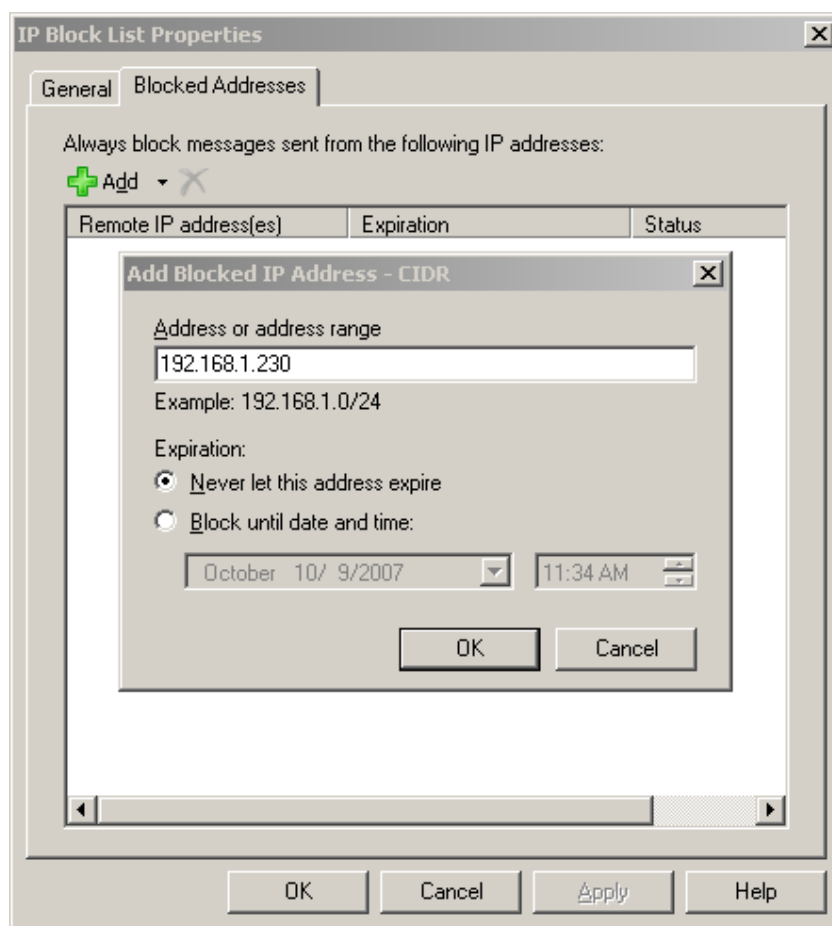
Trên EX01, đăng nhập vào Outlook Web Access với tài khoản Harry, xác nhận Harry đã nhận được message từ Voldermort.

2. Cấu hình **IP Block List** để chặn kết nối từ địa chỉ IP 192.168.1.230

Trong **Organization Configuration Hub Transport**, vào tab **Anti-spam**, nhấn phải vào **IP Block List** rồi chọn **Properties**.



Trong hộp thoại **IP Block List Properties**, vào tab **Blocked Addresses**, nhấn **Add**, rồi nhập **192.168.1.230** vào ô **Address or address range**, nhấn **OK**. Nhấn **OK** trong hộp thoại **IP Block List Properties**.

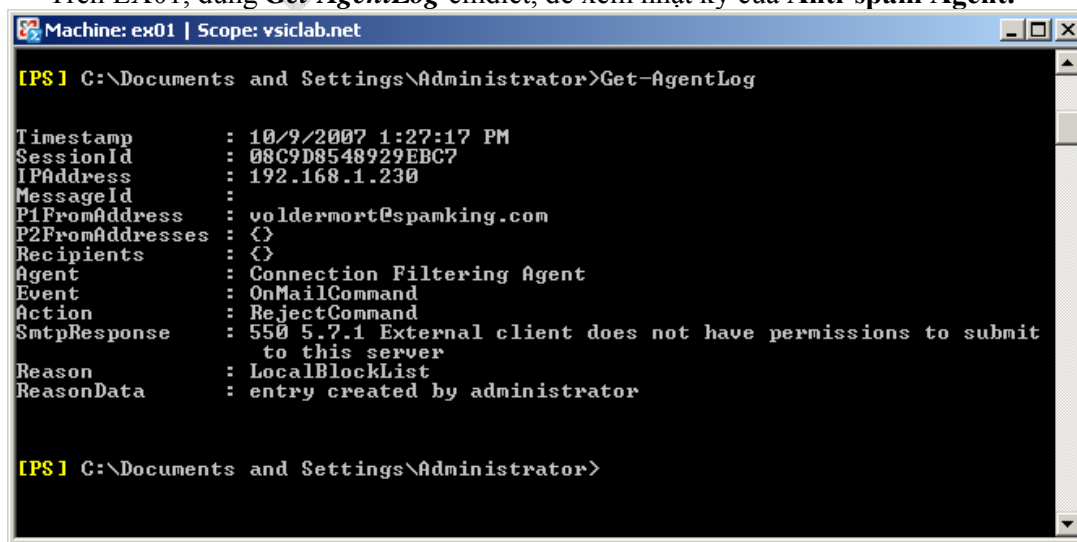


3. Xác nhận **IP Block List** đã được áp dụng

Trên SPAMMER, đăng nhập vào Outlook Express với tài khoản Voldermort, gửi một message đến harry@vsiclab.net với tiêu đề **Test IP Block List – After config**.

Chờ một lát Voldermort sẽ nhận được message báo rằng không thể chuyển message đã gửi cho Harry.

Trên EX01, dùng **Get-AgentLog** cmdlet, để xem nhật ký của **Anti-spam Agent**.



4. Vô hiệu hoá các thiết lập đã thực hiện để chuẩn bị cho bài thực hành tiếp theo.

Cấu hình Connection Filtering với IP Block List Providers

1. Gửi một message từ Voldermort đến Harry. Xác nhận Harry đã nhận được message từ Voldermort.

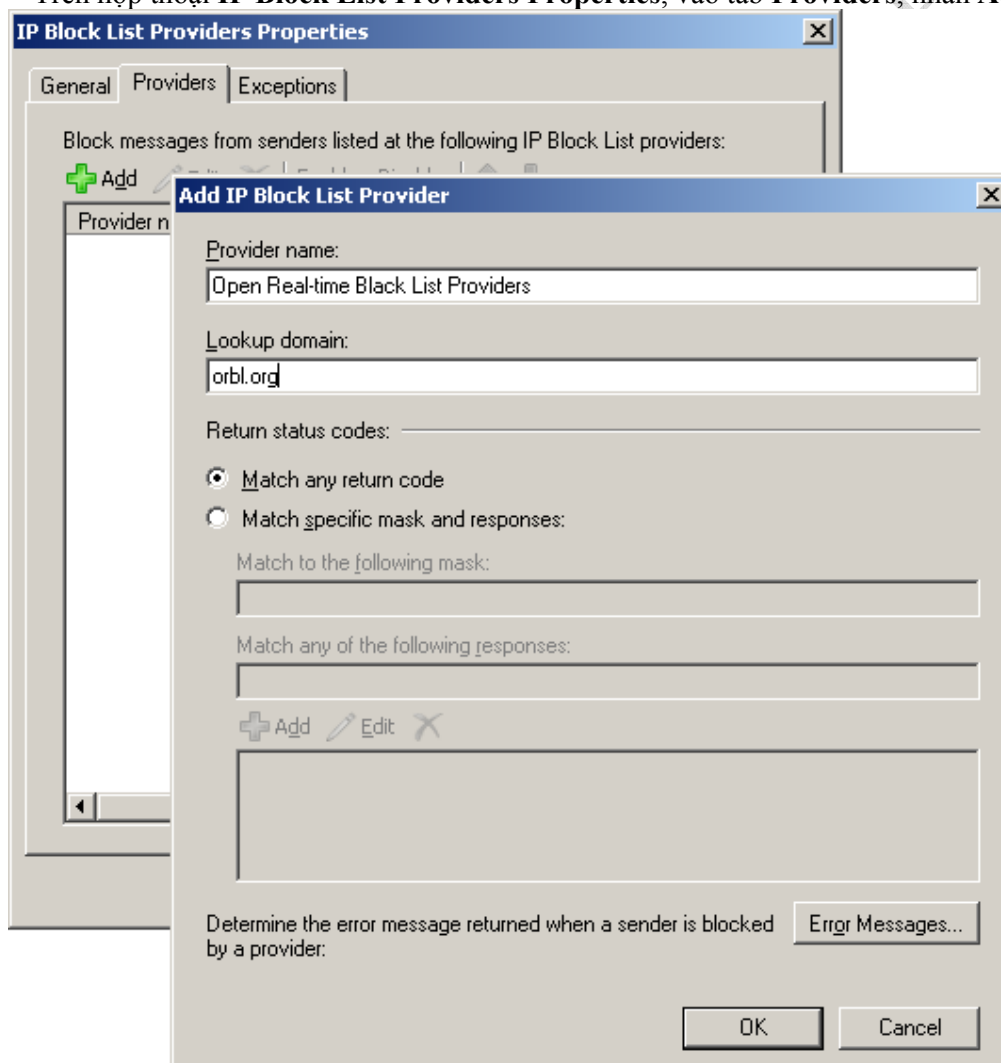
Trên SPAMMER, đăng nhập vào Outlook Express với tài khoản Voldermort, gửi một message đến harry@vsiclab.net với tiêu đề **Test IP Block List Providers – Before config**.

Trên EX01, đăng nhập vào Outlook Web Access với tài khoản Harry, xác nhận Harry đã nhận được message từ Voldermort.

2. Cấu hình **IP Block List Providers** để chặn tất cả message đến từ các địa chỉ mà **Block List Providers** xác nhận là nơi gửi các message spam.

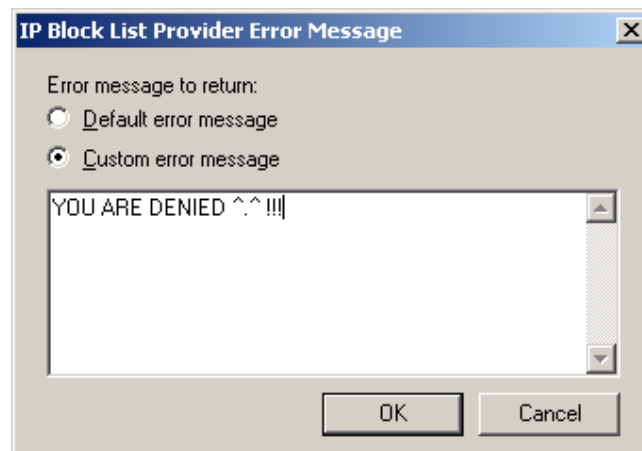
Trong **Organization Configuration\Hub Transport**, vào tab **Anti-spam**, nhấn phải vào **IP Block List Providers** rồi chọn **Properties**.

Trên hộp thoại **IP Block List Providers Properties**, vào tab **Providers**, nhấn **Add**.



Trên hộp thoại Add IP Block List Providers, nhập **Open Real-time Black List Providers** trong **Provider name** và **orbl.org** trong **Lookup domain**. Nhấn **Error Messages**.

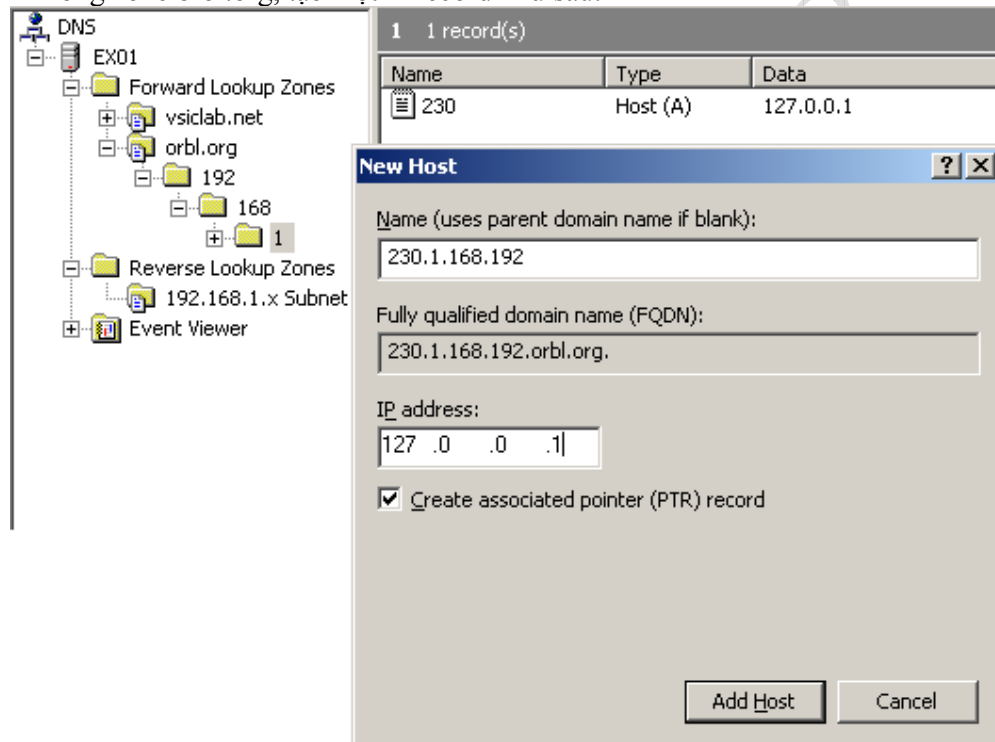
Nhập thông điệp báo lỗi. Rồi nhấn **OK** 3 lần để thoát khỏi hộp thoại cấu hình **IP Block List Providers**.



3. Cấu hình DNS để giả lập làm **Block List Providers**.

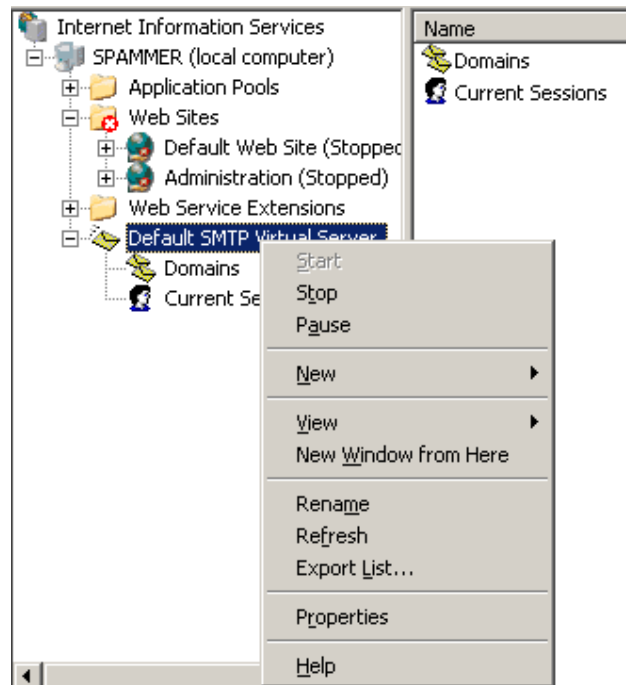
Trên DNS Server tại EX01, tạo một zone mới với tên orbl.org

Trong zone orbl.org, tạo một A record như sau:

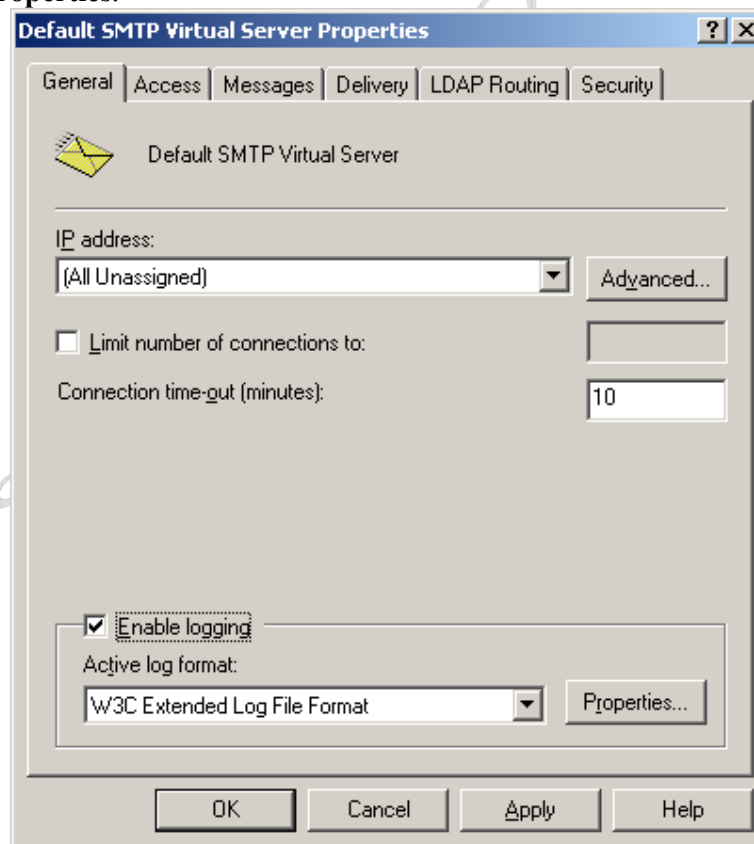


4. Cấu hình ghi nhật ký cho SMTP Virtual Server.

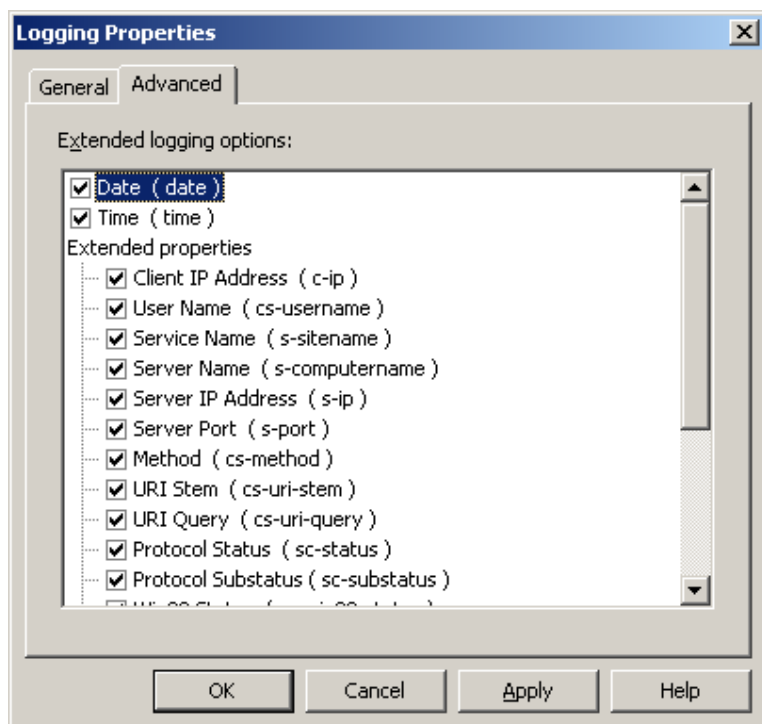
Trên SPAMMER, nhấn phải vào **Default SMTP Virtual Server** trong **Internet Information Service (IIS) Manager**, chọn **Properties**.



Trong hộp thoại **Default SMTP Virtual Server Properties**, chọn **Enable logging**, rồi nhấn **Properties**.



Trong hộp thoại **Logging Properties**, vào tab **Advanced**, chọn các thông tin cần ghi vào nhật ký.



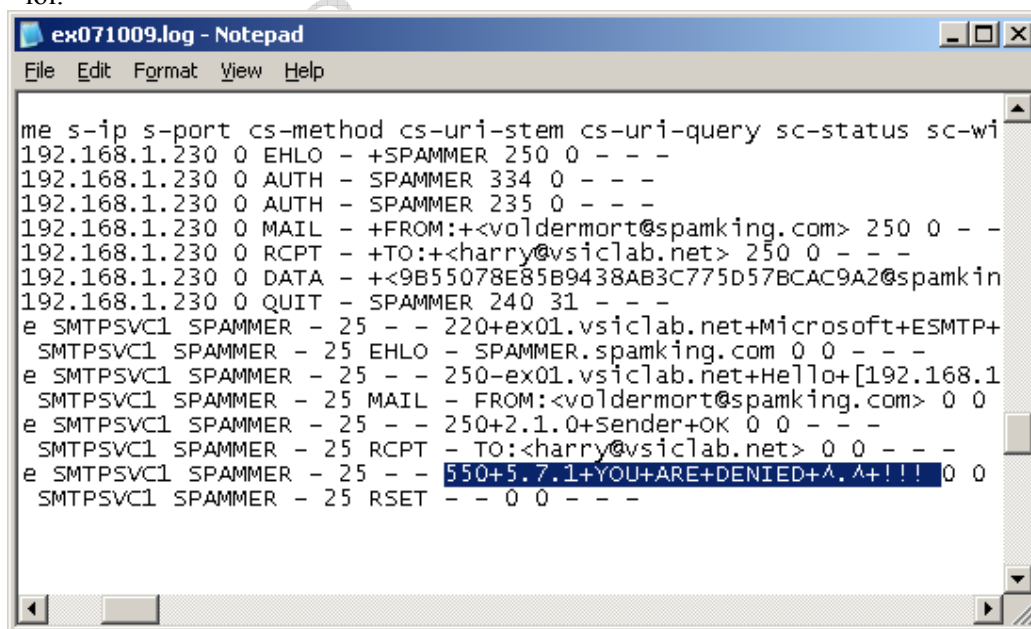
Nhấn **OK** 2 lần để thoát ra khỏi hộp thoại **Default SMTP Virtual Server Properties**

5. Xác nhận **IP Block List Providers** đã được áp dụng

Trên SPAMMER, đăng nhập vào Outlook Express với tài khoản Voldermort, gửi một message đến harry@vsiclab.net với tiêu đề **Test IP Block List Providers – After config**.

Chờ một lát Voldermort sẽ nhận được message báo rằng không thể chuyển message đã gửi cho Harry.

Mở file nhật ký tại **C:\WINDOWS\System32\LogFiles\SMTPSVC1**, xem thông báo lỗi.



6. Vô hiệu hoá các thiết lập đã thực hiện để chuẩn bị cho bài thực hành tiếp theo.

Cấu hình Sender Filtering

1. Gửi một message từ Voldermort đến Harry. Xác nhận Harry đã nhận được message từ Voldermort

Trên SPAMMER, đăng nhập vào Outlook Express với tài khoản Voldermort, gửi một message đến harry@vsiclab.net với tiêu đề **Test Sender Filtering – Before config**.

Trên EX01, đăng nhập vào Outlook Web Access với tài khoản Harry, xác nhận Harry đã nhận được message từ Voldermort.

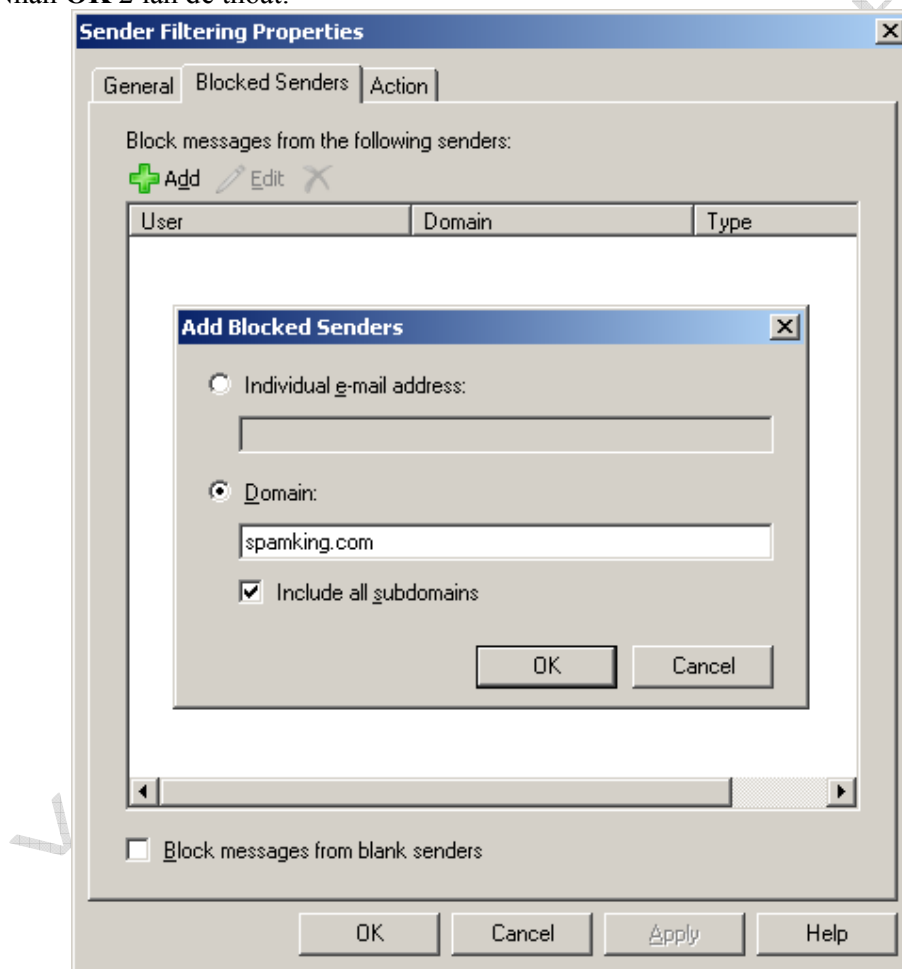
2. Cấu hình **Sender Filtering** để chặn tất cả message đến từ domain **spamking.com**.

Trong **Organization Configuration\Hub Transport**, vào tab **Anti-spam**, nhấn phải vào **Sender Filtering** rồi chọn **Properties**.

Trên hộp thoại **Sender Filtering Properties**, vào tab **Blocked Senders**, nhấn **Add**.

Trong hộp thoại **Add Blocked Senders**, chọn **Domain** rồi nhập vào **spamking.com**.

Nhấn **OK** 2 lần để thoát.



3. Xác nhận **Sender Filtering** đã được áp dụng

Trên SPAMMER, đăng nhập vào **Outlook Express** với tài khoản Voldermort, gửi một message đến harry@vsiclab.net với tiêu đề **Test Sender Filtering – After config**.

Chờ một lát Voldermort sẽ nhận được message báo rằng không thể chuyển message đã gửi cho Harry.

Mở file nhật ký tại **C:\WINDOWS\System32\LogFiles\SMTPSVC1**, xem thông báo lỗi.

```

s-method cs-uri-stem cs-uri-query sc-status sc-win32-status cs(Us
EHLO - +SPAMMER 250 0 - - -
AUTH - SPAMMER 334 0 - - -
AUTH - SPAMMER 235 0 - - -
MAIL - +FROM:+<voldermort@spamking.com> 250 0 - - -
RCPT - +TO:+<harry@vsiclab.net> 250 0 - - -
DATA - +<39461E1E07414702B16FE7A820753565@spamking.com> 250 0 - -
QUIT - SPAMMER 240 78 - - -
ER - 25 - - 220+ex01.vsiclab.net+Microsoft+ESMTP+MAIL+Service+rea
R - 25 EHLO - SPAMMER.spamking.com 0 0 - - -
ER - 25 - - 250-ex01.vsiclab.net+Hello+[192.168.1.230] 0 0 - - -
R - 25 MAIL - FROM:<voldermort@spamking.com> 0 0 - - -
ER - 25 - - 554+5.1.0+Sender+denied 0 0 - - -
R - 25 QUIT - - 0 0 - - -
ER - 25 - - 221+2.0.0+Service+closing+transmission+channel 0 0 -

```

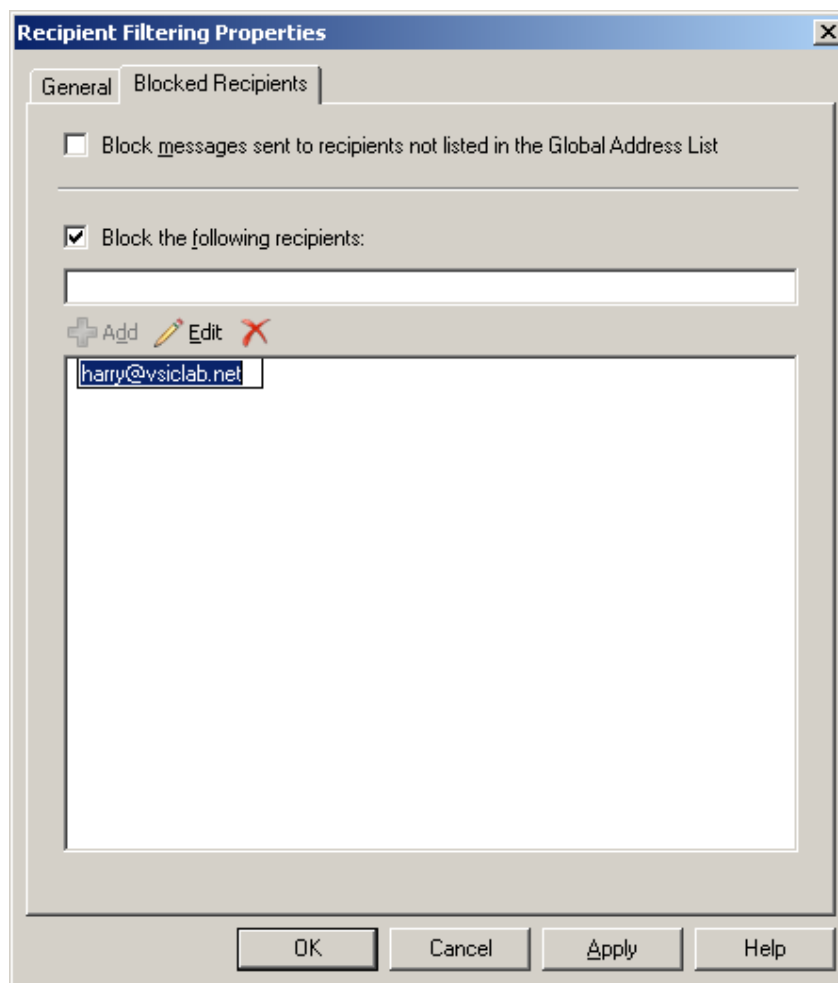
4. Vô hiệu hoá các thiết lập đã thực hiện để chuẩn bị cho bài thực hành tiếp theo.

Cấu hình Recipient Filtering

1. Cấu hình Recipient Filtering để chặn tất cả message gửi đến Harry.

Trong **Organization Configuration\Hub Transport**, vào tab **Anti-spam**, nhấn phải vào **Recipient Filtering** rồi chọn **Properties**.

Trên hộp thoại **Recipient Filtering Properties**, vào tab **Blocked Recipients**, chọn **Block the following recipient**, nhập **harry@vsiclab.net**, rồi nhấn **OK**.



2. Xác nhận **Recipient Filtering** đã được áp dụng

Trên SPAMMER, đăng nhập vào Outlook Express với tài khoản Voldermort, gửi một message đến `harry@vsiclab.net` và `ronald@vsiclab.net` với tiêu đề **Test Recipient Filtering**.

Chờ một lát Voldermort sẽ nhận được message báo rằng không thể chuyển message đã gửi cho Harry.

Trên EX01, đăng nhập vào Outlook Web Access với tài khoản Harry, xác nhận Harry không nhận được message từ Voldermort.

Trên EX01, đăng nhập vào Outlook Web Access với tài khoản Ronald, xác nhận Ronald đã nhận được message từ Voldermort.

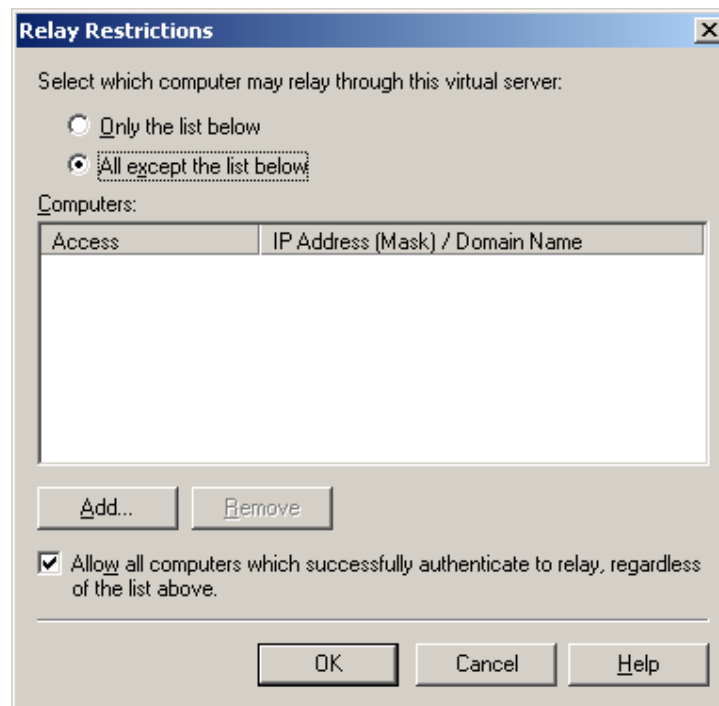
3. Vô hiệu hoá các thiết lập đã thực hiện để chuẩn bị cho bài thực hành tiếp theo.

Cấu hình Sender ID

1. Cho phép Relay trên SPAMMER.

Vào tab **Access** trong hộp thoại **Default SMTP Virtual Server Properties**. Nhấn **Relay**.

Trong hộp thoại **Relay Restrictions**, chọn **All except the list below**, rồi nhấn OK 2 lần để thoát ra khỏi hộp thoại **Default SMTP Virtual Server Properties**.



2. Sử dụng SMTP Relay trên SPAMMER để giả mạo Ronald gửi một message cho Harry. Xác nhận Harry đã nhận được message giả mạo từ Ronald.

Telnet vào port 25 trên SPAMMER và thực hiện các lệnh sau:

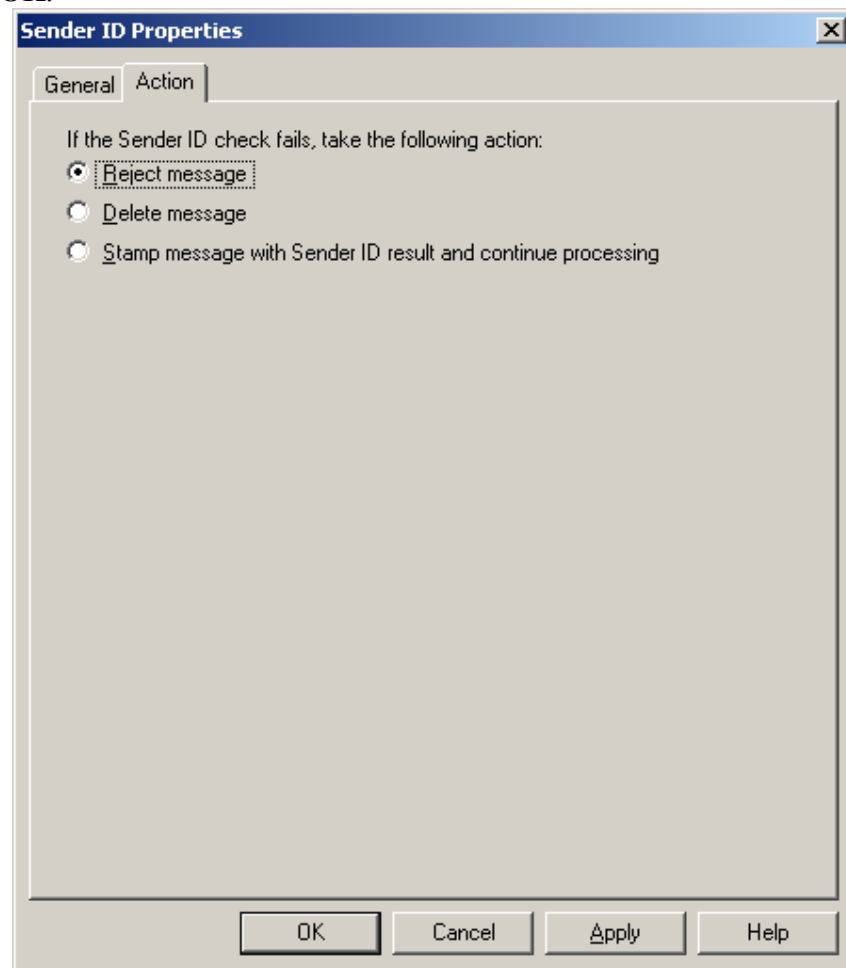
```
220 SPAMMER.spamking.com Microsoft ESMTP MAIL Service, Version: 6.0.3790.3959
ready at Wed, 10 Oct 2007 14:37:48 +0700
HELO vsiclab.net
250 SPAMMER.spamking.com Hello [192.168.1.230]
MAIL FROM: ronald@vsiclab.net
250 2.1.0 ronald@vsiclab.net....Sender OK
RCPT TO: harry@vsiclab.net
250 2.1.5 harry@vsiclab.net
DATA
354 Start mail input; end with <CRLF>.<CRLF>
From: Ronald Weasley
To: Harry Potter
Subject: Test fake message
Fake Message.
.
250 2.6.0 <SPAMMERZDgC81TbdkSm00000003@SPAMMER.spamking.com> Queued
mail for delivery
quit
221 2.0.0 SPAMMER.spamking.com Service closing transmission channel
Connection to host lost.
```

Trên EX01, đăng nhập vào **Outlook Web Access** với tài khoản Harry, xác nhận Harry đã nhận được message giả mạo.

3. Cấu hình **Sender ID** để yêu cầu xác nhận chỉ có Server với địa chủ IP 192.168.1.220 mới được message từ domain vsiclab.net.

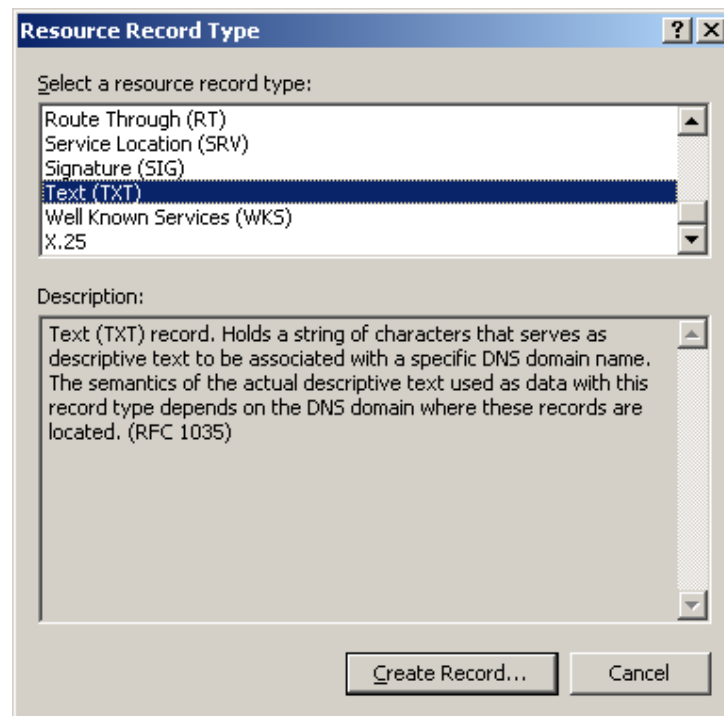
Trong **Organization Configuration\Hub Transport**, vào tab **Anti-spam**, nhấn phải vào **Sender ID** rồi chọn **Properties**.

Trên hộp thoại **Sender ID Properties**, vào tab **Action**, chọn **Reject message**, rồi nhấn **OK**.

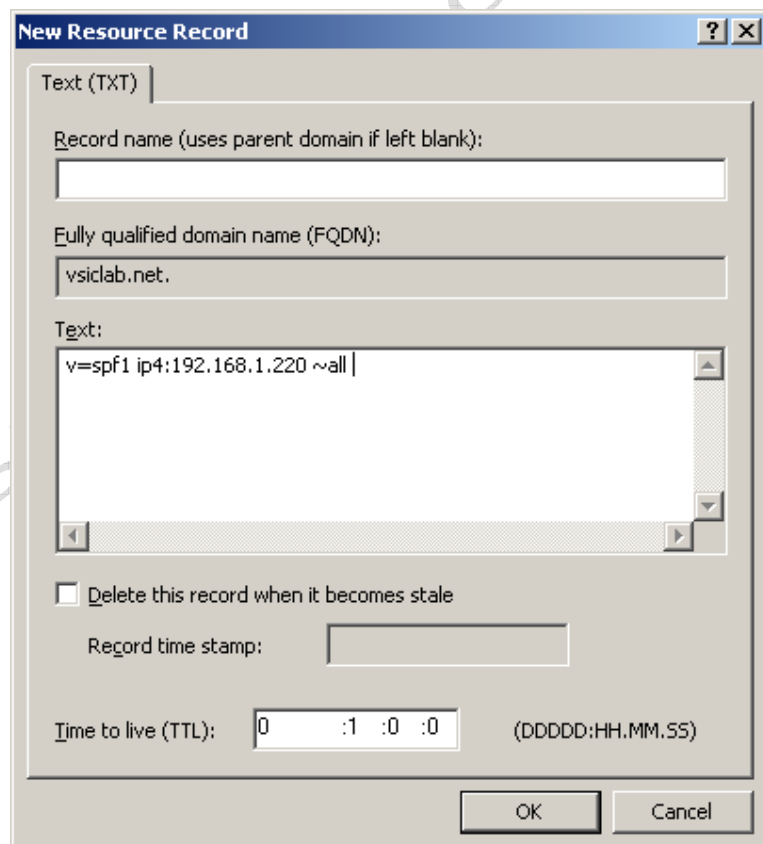


Trên EX01, vào **DNS Management Console**, tạo **SPF record**. Nhấn phải vào vsiclab.net zone, chọn Other New Record.

Chọn **Text (TXT)** trong hộp thoại **Resource Record Type**, rồi nhấn **Create Record**.



Trong hộp thoại New Resource Record, nhập **v=spf1 ip4:192.168.1.220 ~all** vào ô **Text**:



3. Trên SPAMMER, gửi một message giả mạo từ Ronald đến Harry. Xác nhận message bị từ chối.

Telnet vào port 25 trên SPAMMER và thực hiện các lệnh sau:

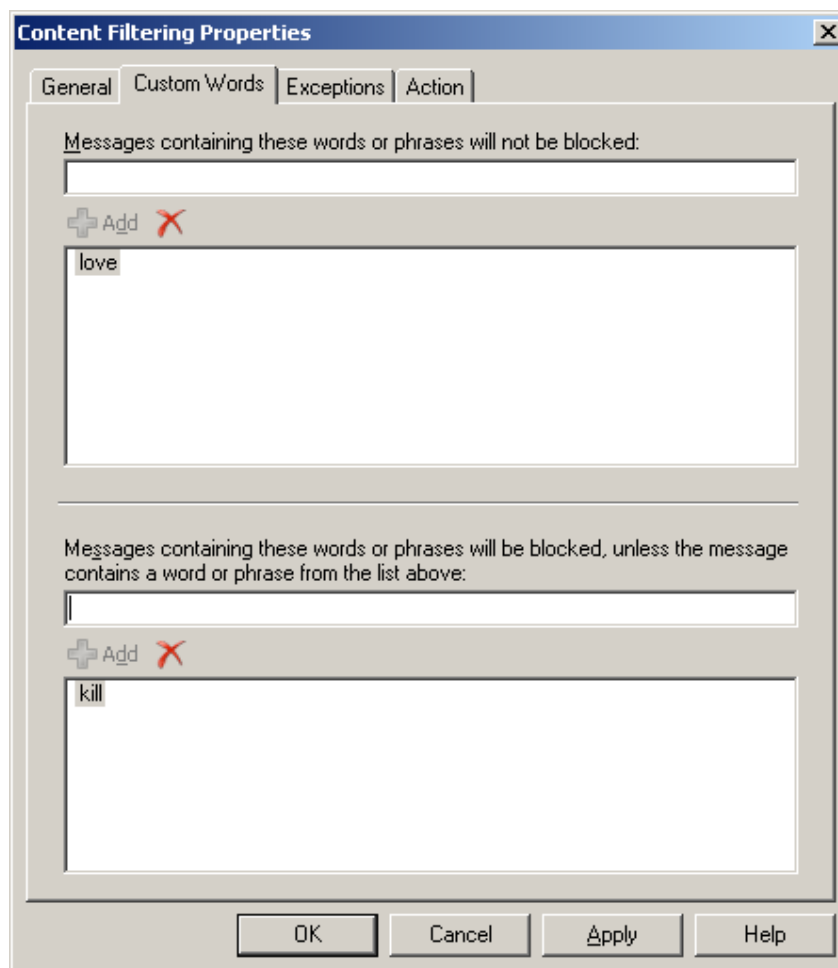
```
220 SPAMMER.spamking.com Microsoft ESMTP MAIL Service, Version: 6.0.3790.3959
ready at Wed, 10 Oct 2007 14:37:48 +0700
HELO vsiclab.net
250 SPAMMER.spamking.com Hello [192.168.1.230]
MAIL FROM: ronald@vsiclab.net
250 2.1.0 ronald@vsiclab.net....Sender OK
RCPT TO: harry@vsiclab.net
250 2.1.5 harry@vsiclab.net
DATA
354 Start mail input; end with <CRLF>.<CRLF>
From: Ronald Weasley
To: Harry Potter
Subject: Test fake message
Fake Message.
.
250 2.6.0 <SPAMMERZDgC81TbdkSm00000003@SPAMMER.spamking.com> Queued
mail for delivery
quit
221 2.0.0 SPAMMER.spamking.com Service closing transmission channel
Connection to host lost.
```

Cấu hình Content Filtering

1. Cấu hình Recipient **Filtering** để chặn tất cả message có chứa từ khoá “**kill**”, ngoại trừ những message có từ khoá “love”.

Trong **Organization Configuration\Hub Transport**, vào tab **Anti-spam**, nhấn phải vào **Content Filtering** rồi chọn **Properties**.

Trên hộp thoại **Content Filtering Properties**, vào tab **Custom Words**, nhập các từ **kill** và **love** vào các ô tương ứng rồi nhấn **Add**. Nhấn **OK** để kết thúc cấu hình.



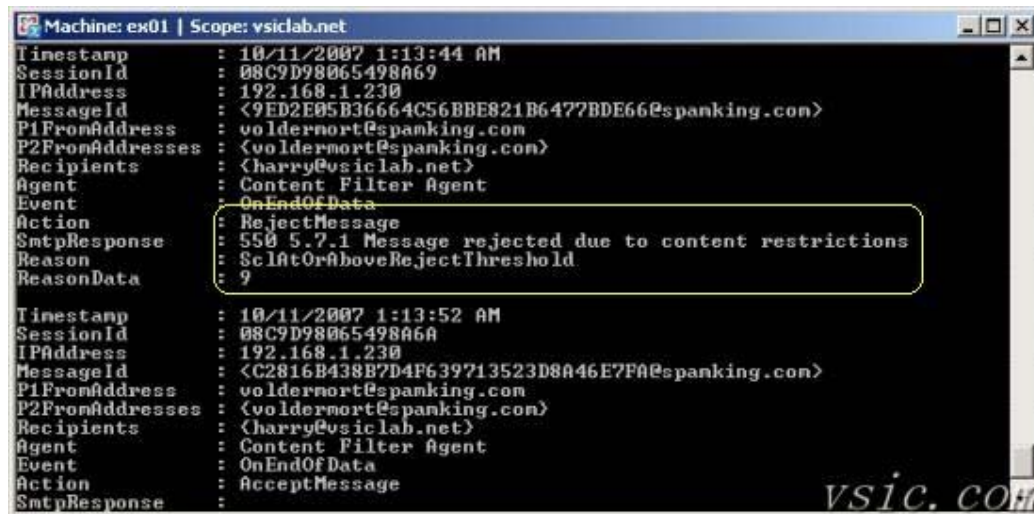
2. Xác nhận **Content Filtering** đã được áp dụng

Trên SPAMMER, đăng nhập vào Outlook Express với tài khoản Voldermort, gửi một message đến harry@vsiclab.net tiêu đề **Test Content Filtering – Block message** và nội dung là : ***I will kill you.***

Gửi tiếp một message đến Harry với tiêu đề **Test Content Filtering – Allow message** và nội dung là : ***I will not kill you because I love you.***

Trên EX01, đăng nhập vào Outlook Web Access với tài khoản Harry, xác nhận Harry chỉ nhận được message có tiêu đề **Test Content Filtering – Allow message.**

Trên EX01, dùng **Get-AgentLog cmdlet**, để xem nhật ký của **Anti-spam Agent**.



```
Machine: ex01 | Scope: vsiclab.net
Timestamp : 10/11/2007 1:13:44 AM
SessionId : 08C9D98065498A69
IPAddress : 192.168.1.230
MessageId : <9ED2E05B36664C56BBE821B6477BDE66@spanking.com>
P1FromAddress : voldermort@spanking.com
P2FromAddresses : <voldermort@spanking.com>
Recipients : <harry@vsiclab.net>
Agent : Content Filter Agent
Event : OnEndOfData
Action : RejectMessage
SmtprResponse : 550 5.7.1 Message rejected due to content restrictions
Reason : SclAtOrAboveRejectThreshold
ReasonData : 9

Timestamp : 10/11/2007 1:13:52 AM
SessionId : 08C9D98065498A6A
IPAddress : 192.168.1.230
MessageId : <C2816B438B7D4F639713523D8A46E7FA@spanking.com>
P1FromAddress : voldermort@spanking.com
P2FromAddresses : <voldermort@spanking.com>
Recipients : <harry@vsiclab.net>
Agent : Content Filter Agent
Event : OnEndOfData
Action : AcceptMessage
SmtprResponse :
```

3. Vô hiệu hoá các thiết lập đã thực hiện để chuẩn bị cho bài thực hành tiếp theo.

Bài tập 2 Sử dụng các tính năng Anti-Virus

Cấu hình Attachment Filtering

Trong bài tập này, bạn sẽ cấu hình **Attachment Filtering** để lọc các message chứa file đính kèm có phần mở rộng **.vmp**.

Chuẩn bị

Bài thực hành này cần 3 server

EX01: DNS, DC, Exchange 2007 (Mailbox Server, Client Access, Hub Transport), địa chỉ IP 192.168.1.220.

Edge1: Exchange 2007 (Edge Transport), địa chỉ IP 192.168.1.222.

SPAMMER: DNS, SMTP Service, POP3 Service, địa chỉ IP 192.168.1.230

1. Gửi một message từ Voldermort đến Harry. Xác nhận Harry đã nhận được message từ Voldermort

Trên SPAMMER, tạo một file **test.vmp** có nội dung bất kỳ.

Trên SPAMMER, đăng nhập vào Outlook Express với tài khoản Voldermort, gửi một message đến **harry@vsiclab.net** với tiêu đề **Test Attachment Filtering– Before config** và đính kèm file **test.vmp**

Trên EX01, đăng nhập vào Outlook Web Access với tài khoản Harry, xác nhận Harry đã nhận được message từ Voldermort.

2. Xác nhận tính năng **Attachment Filtering** đã được kích hoạt và kích hoạt **Attachment Filtering** nếu tính năng này chưa được kích hoạt trước đó.

Trên Edge1, trong **Exchange Management Shell**, sử dụng **Get-TransportAgent cmdlet** để xác nhận Attachment Filtering đã được kích hoạt.

```
Machine: edge1 | Scope: View Entire Forest
[PS] C:\>
[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

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

Nếu **Attachment Filtering** chưa được kích hoạt có thể sử dụng **Enable-TransportAgent -Identity "Attachment Filtering Agent"** cmdlet để kích hoạt.

3. Cấu hình **Attachment Filtering** để lọc các message chứa file đính kèm có phần mở rộng là **.vmp**.

Trên Edge1, trong **Exchange Management Shell**, nhập **Add-AttachmentFilterEntry -Name *.vmp -Type FileName**, rồi nhấn Enter.

```
Machine: edge1 | Scope: View Entire Forest
[PS] C:\>
[PS] C:\>Add-AttachmentFilterEntry -Name *.vmp -Type Filename

Type Name Identity
-----
Filename *.vmp FileName:*.vmp

[PS] C:\>
```

Cấu hình thông điệp phản hồi cho người gửi bằng lệnh **Set-AttachmentFilterListConfig -Action Reject -RejectResponse "The attachment you included in your e-mail message was not allowed. Your e-mail message cannot be delivered. Please remove the e-mail attachment, and send your message again."** trong **Exchange Management Shell**.

4. Xác nhận **Attachment Filtering** đã được áp dụng

Trên SPAMMER, đăng nhập vào Outlook Express với tài khoản Voldermort, gửi một message đến harry@vsiclab.net với tiêu đề **Test Attachment Filtering– After config** và đính kèm file **test.vmp**

Chờ một lát Voldermort sẽ nhận được message báo rằng không thể chuyển message đã gửi cho Harry.

Mở file nhật ký tại **C:\WINDOWS\System32\LogFiles\SMTPSVC1**, xem thông báo lỗi.

```
ex071011.log - Notepad
File Edit Format View Help
250-edge1.vsiclab.net+Hello+[192.168.1.230] 0 0 - - -
2007-10-11 06:42:46 192.168.1.222 outboundConnectionCommand
SMTPSVC1 SPAMMER - 25 MAIL -
FROM:<voldermort@spamking.com>+SIZE=1287 0 0 - - -
2007-10-11 06:42:46 192.168.1.222 outboundConnectionResponse
SMTPSVC1 SPAMMER - 25 - - 250+2.1.0+Sender+OK 0 0 - - -
2007-10-11 06:42:46 192.168.1.222 outboundConnectionCommand
SMTPSVC1 SPAMMER - 25 RCPT - TO:<harry@vsiclab.net> 0 0 - - -
2007-10-11 06:42:46 192.168.1.222 outboundConnectionResponse
SMTPSVC1 SPAMMER - 25 - - 250+2.1.5+Recipient+OK 0 0 - - -
2007-10-11 06:42:46 192.168.1.222 outboundConnectionCommand
SMTPSVC1 SPAMMER - 25 BDAT - 1287+LAST 0 0 - - -
2007-10-11 06:42:54 192.168.1.222 outboundConnectionResponse
SMTPSVC1 SPAMMER - 25 - -
550+5.7.1+The+attachment+you+included+in+your+e-mail+message+was+
not+allowed.+Your+e-mail+message+cannot+be+delivered.+Please+remo
ve+the+e-mail+attachment,+and+send+your+message+again. 0 0 - - -
2007-10-11 06:42:54 192.168.1.222 outboundConnectionCommand
SMTPSVC1 SPAMMER - 25 QUIT - - 0 0 - - -
2007-10-11 06:42:54 192.168.1.222 outboundConnectionResponse
SMTPSVC1 SPAMMER - 25 - -
```

5. Vô hiệu hoá các thiết lập đã thực hiện để chuẩn bị cho bài thực hành tiếp theo.

Module 2 Configuring Edge Transport Servers

Bài tập 1 Hiện thực Edge Transport Server Role

Các công việc chính của bài tập này bao gồm:

- Sử dụng Security Configuration Wizard để bảo vệ Edge Transport server
- Cấu hình EdgeSync

Chuẩn bị

Bài thực hành này cần 2 server

EX01: DNS, DC, Exchange 2007 (Mailbox Server, Client Access, Hub Transport), địa chỉ IP 192.168.1.220.

Edge1: Exchange 2007 (Edge Transport), địa chỉ IP 192.168.1.222.

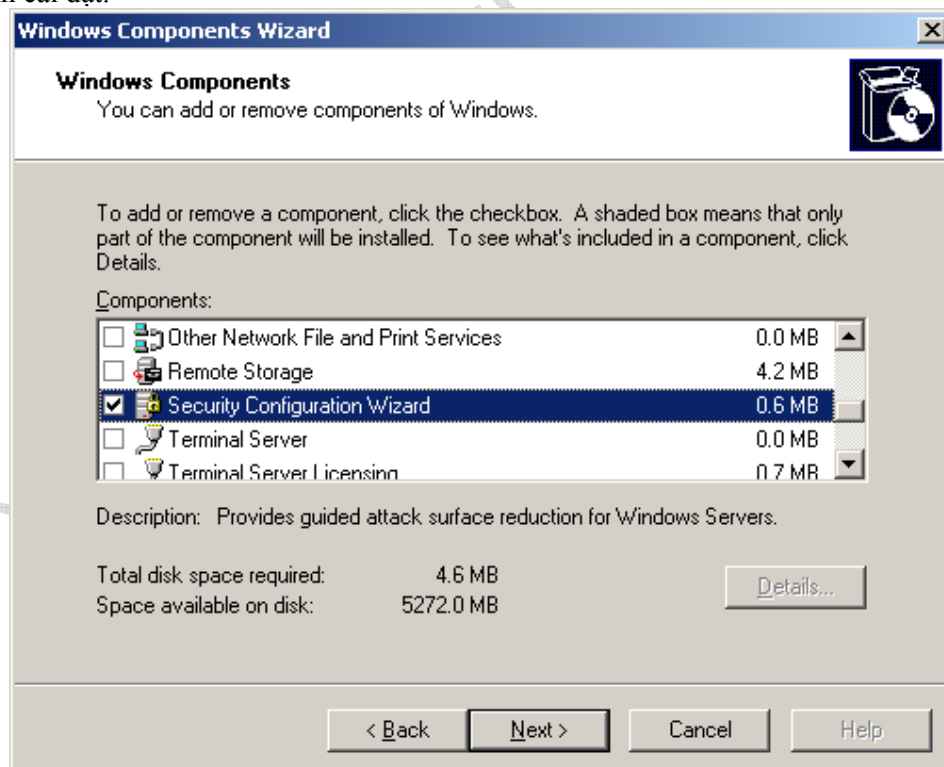
Sử dụng Security Configuration Wizard để bảo vệ Edge Transport server

1. Cài đặt Security Configuration Wizard

Trên Edge1 vào **Start/Control Panel**, và nhấn **Add or Remove Programs**.

Nhấn **Add/Remove Windows Components**.

Trên trang **Windows Components**, trong danh sách **Components**, chọn lựa chọn **Security Configuration Wizard**, rồi nhấn **Next**. Sau đó, nhấn **Finish** để hoàn tất quá trình cài đặt.



Đóng **Add or Remove Programs**.

2. Đăng ký Exchange Server 2007 Edge Transport server role extension

Mở Windows Explorer, di chuyển vào **C:\Program Files\Microsoft**

Exchange Server\Scripts. Sao chép file **Exchange2007Edge.xml** vào thư mục

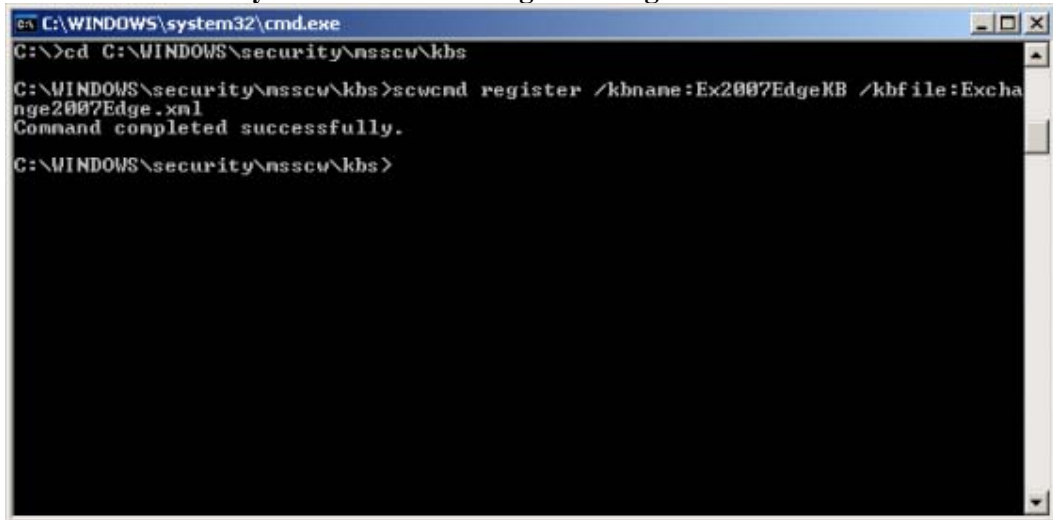
C:\Windows\security\msscw\kbs. Đóng Windows Explorer.

Mở cửa sổ Command Prompt, gõ lệnh dùng để sử dụng **Security Configuration**

Wizard command-line tool để đăng ký Exchange Server 2007 Edge Transport server role extension với local security configuration database: **scwcmd register**

/kbname:Ex2007EdgeKB /kbfile:

c:\Windows\security\msscw\kbs\Exchange2007Edge.xml



```
on C:\WINDOWS\system32\cmd.exe
C:\>cd C:\WINDOWS\security\msscw\kbs
C:\WINDOWS\security\msscw\kbs>scwcmd register /kbname:Ex2007EdgeKB /kbfile:Exchange2007Edge.xml
Command completed successfully.
C:\WINDOWS\security\msscw\kbs>
```

Đóng cửa sổ Command Prompt.

3. Cấu hình bảo mật Edge Transport Server với **Security Configuration Wizard**.

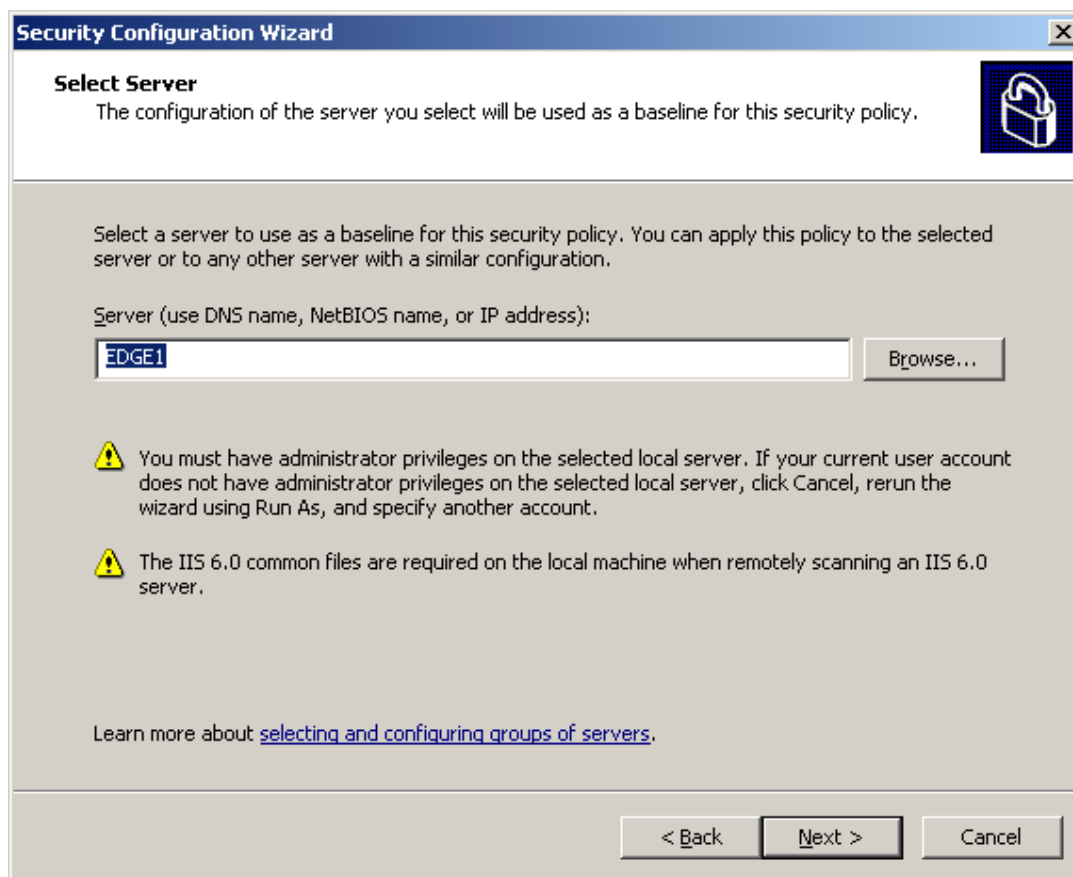
Mở **Start\Administrative Tools\Security Configuration Wizard**.

Trên **Welcome to the Security Configuration Wizard**, nhấn **Next**.

Trên trang **Configuration Action**, chọn **Create a new security policy**, nhấn **Next**.

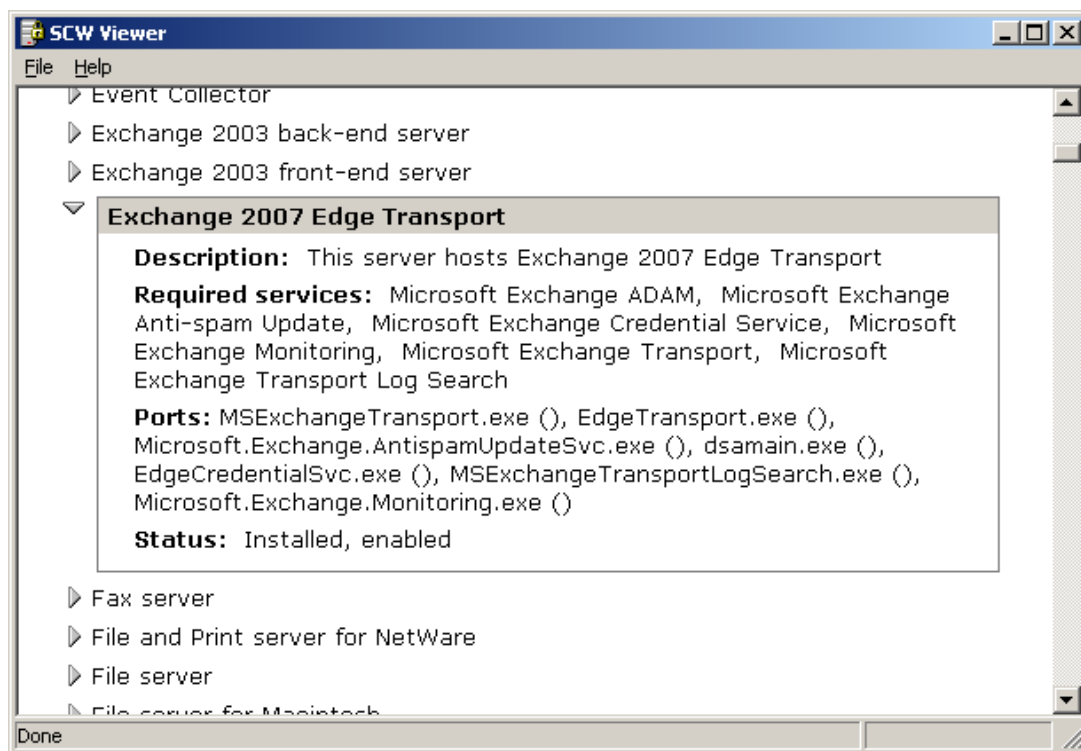


Trên trang **Select Server**, nhấn **Next**.



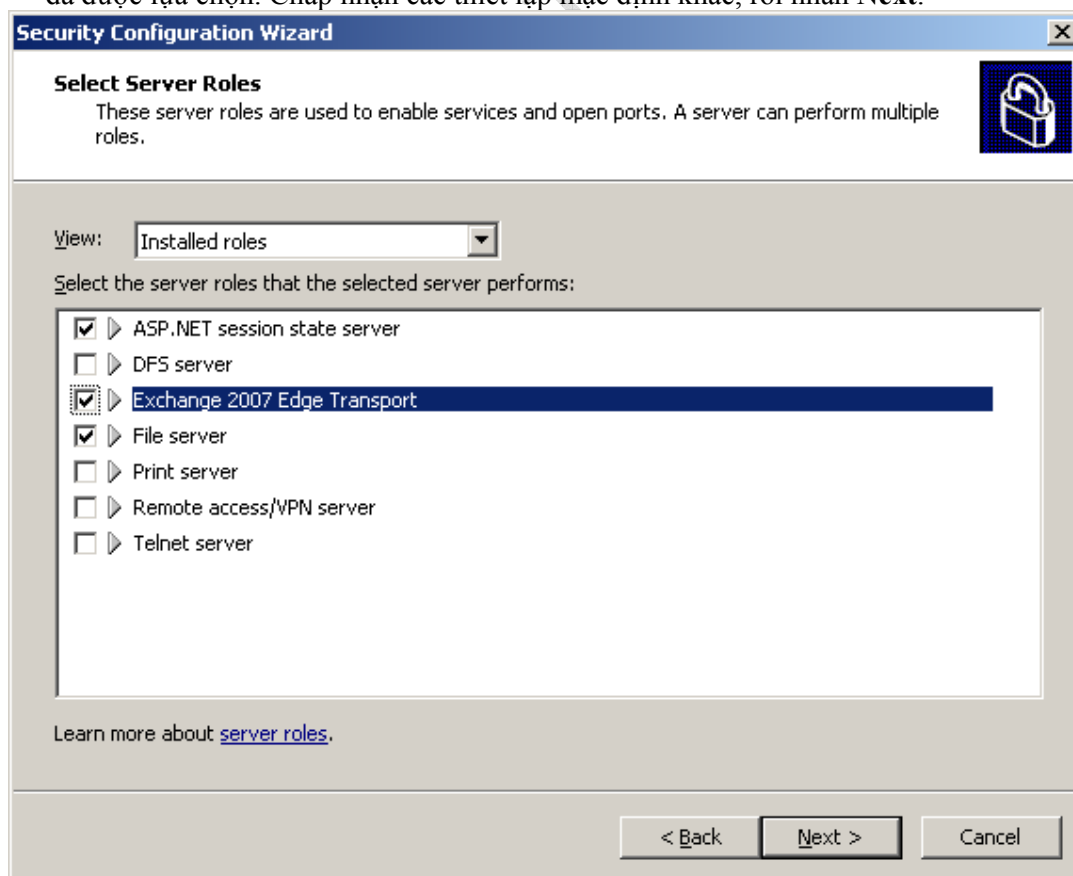
Trên trang **Processing Security Configuration Database**, nhấn **View Configuration Database**.

Mở node Exchange 2007 Edge Transport và kiểm tra nó đã được cài đặt và kích hoạt. Xem lại các dịch vụ yêu cầu và các port trên role này. Đóng cửa sổ **SCW Viewer**, rồi nhấn **Next**.



Trên trang **Role-Based Service Configuration**, nhấn **Next**.

Trên trang **Select Server Roles**, xác nhận Exchange 2007 Edge Transport server role đã được lựa chọn. Chấp nhận các thiết lập mặc định khác, rồi nhấn **Next**.

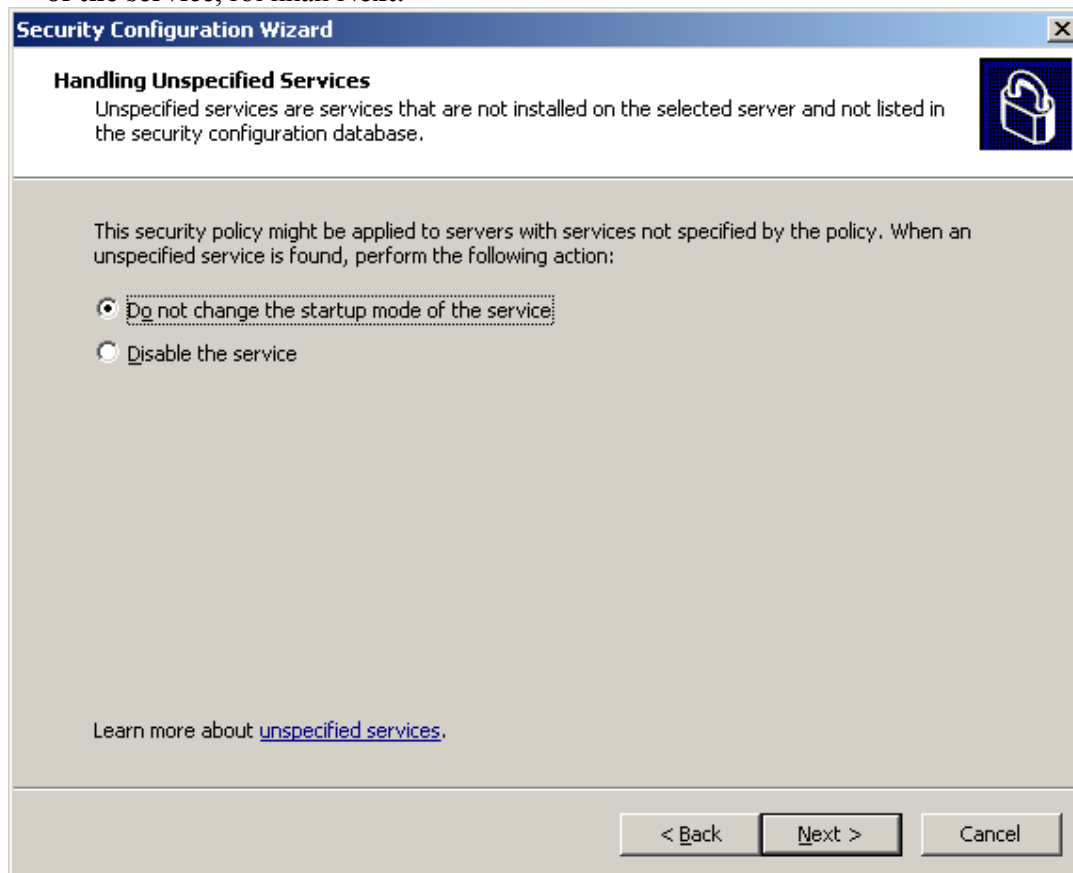


Trên trang **Select Client Features**, nhấn **Next**.

Trên trang **Select Administration and Other Options**, nhấn **Next**.

Trên trang **Select Additional Services**, xem lại các dịch vụ bổ sung mà wizard đã phát hiện trên server, nhấn **Next**.

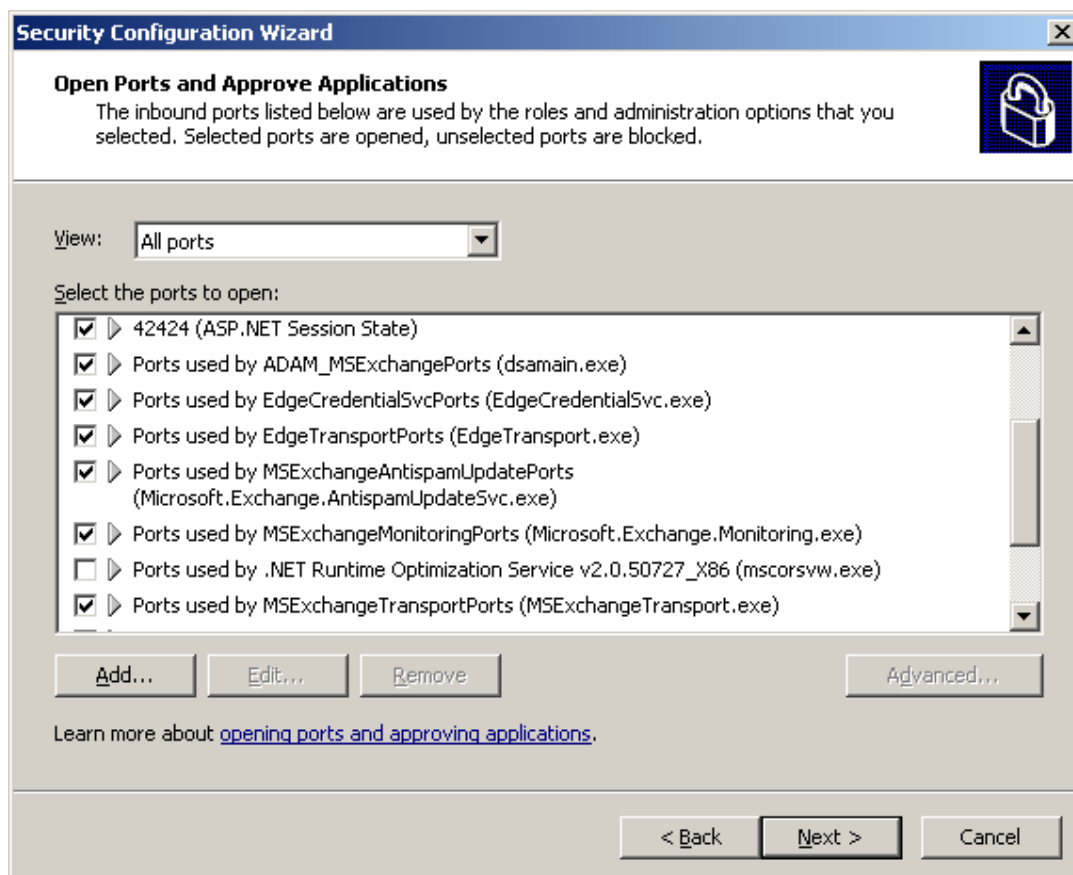
Trên trang **Handling Unspecified Services**, chọn **Do not change the startup mode of the service**, rồi nhấn **Next**.



Trên trang **Confirm Service Changes**, xem lại các cấu hình dịch vụ sẽ được thay đổi, nhấn **Next**.

Trên trang **Network Security**, nhấn **Next**.

Trên trang **Open Ports and Approve Applications**, xem lại các port sẽ được mở. Ghi chú các mục của các ứng dụng được chấp thuận mà liên quan đến các tiến trình và process Exchange sử dụng. Các ứng dụng được chấp thuận được sử dụng như là một thay thế cho các port tương ứng, để các tiến trình hay dịch vụ có thể mở bất kỳ port nào theo yêu cầu.



Trên trang **Open Ports and Approve Applications**, nhấn **Next**.

Trên trang **Confirm Port Configuration**, nhấn **Next**.

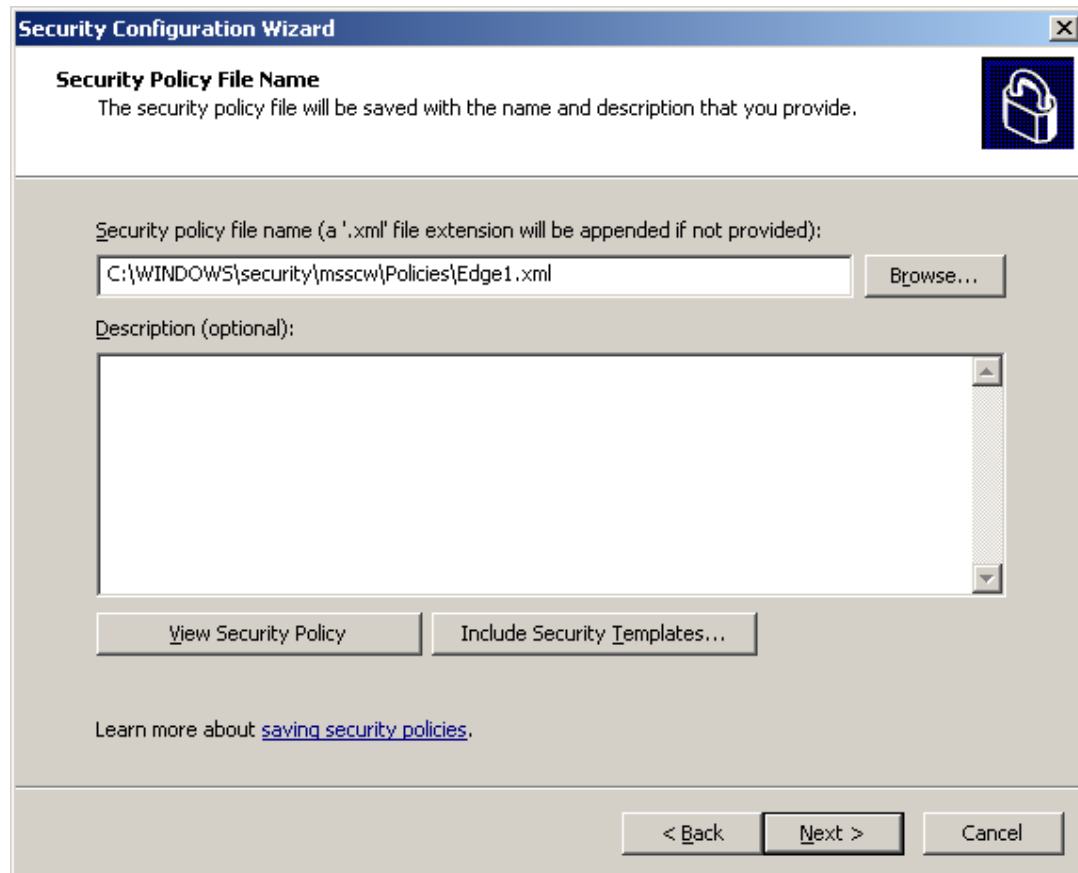
Trên trang **Registry Settings**, chọn **Skip this section**, và nhấn **Next**.

Trên trang **Audit Policy**, chọn **Skip this section**, và nhấn **Next**.

Trên trang **Save Security Policy**, nhấn **Next**.

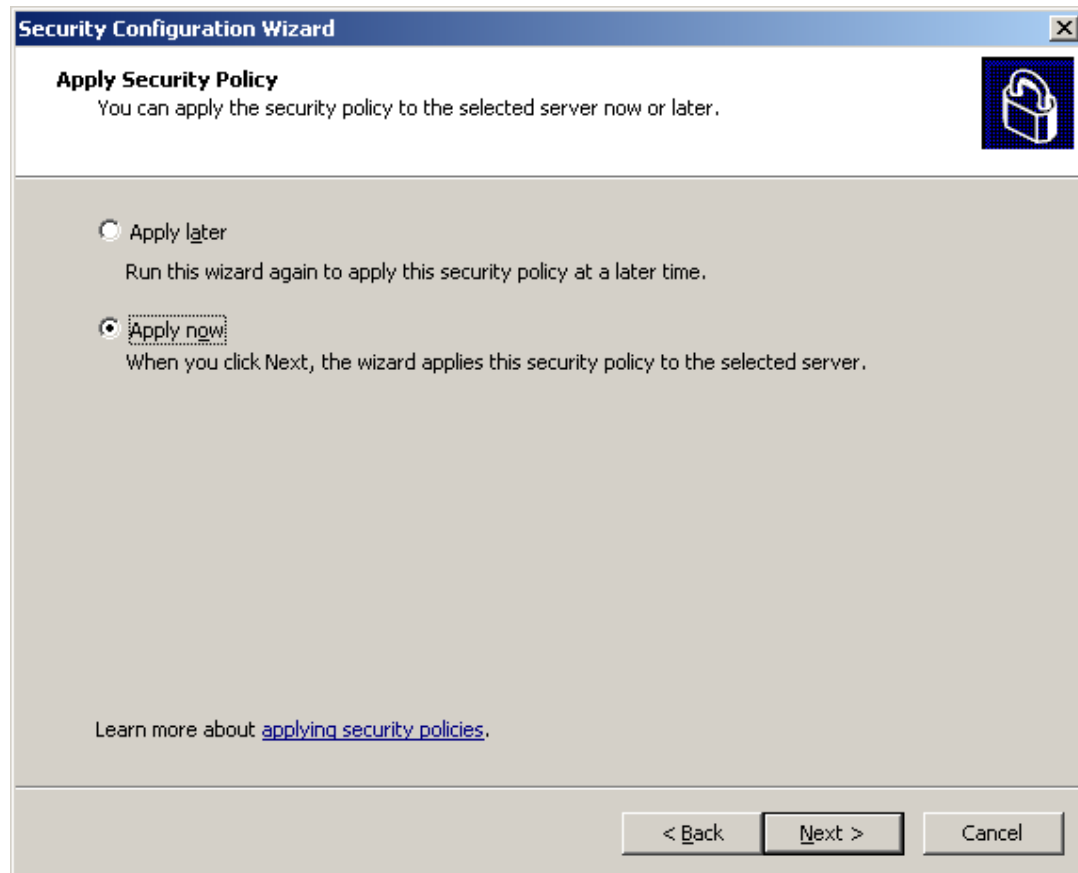
Trên trang **Security Policy File Name**, nhập tên file policy

C:\windows\security\mssecw\policies\Edge1.xml. Nhấn **Next**.



The screenshot shows the 'Security Configuration Wizard' window. It has a title bar with a close button. The main area is titled 'Security Policy File Name' and contains the text: 'The security policy file will be saved with the name and description that you provide.' Below this is a text box for the 'Security policy file name' with the value 'C:\WINDOWS\security\msscw\Policies\Edge1.xml' and a 'Browse...' button. There is also a 'Description (optional):' label followed by a large empty text area. At the bottom of the main area are two buttons: 'View Security Policy' and 'Include Security Templates...'. Below these is a link: 'Learn more about [saving security policies](#).' At the very bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

Trong hộp thoại **Security Configuration Warning**, nhấn **OK**.
Trên trang **Apply Security Policy**, nhấn **Apply now**, rồi nhấn **Next**.



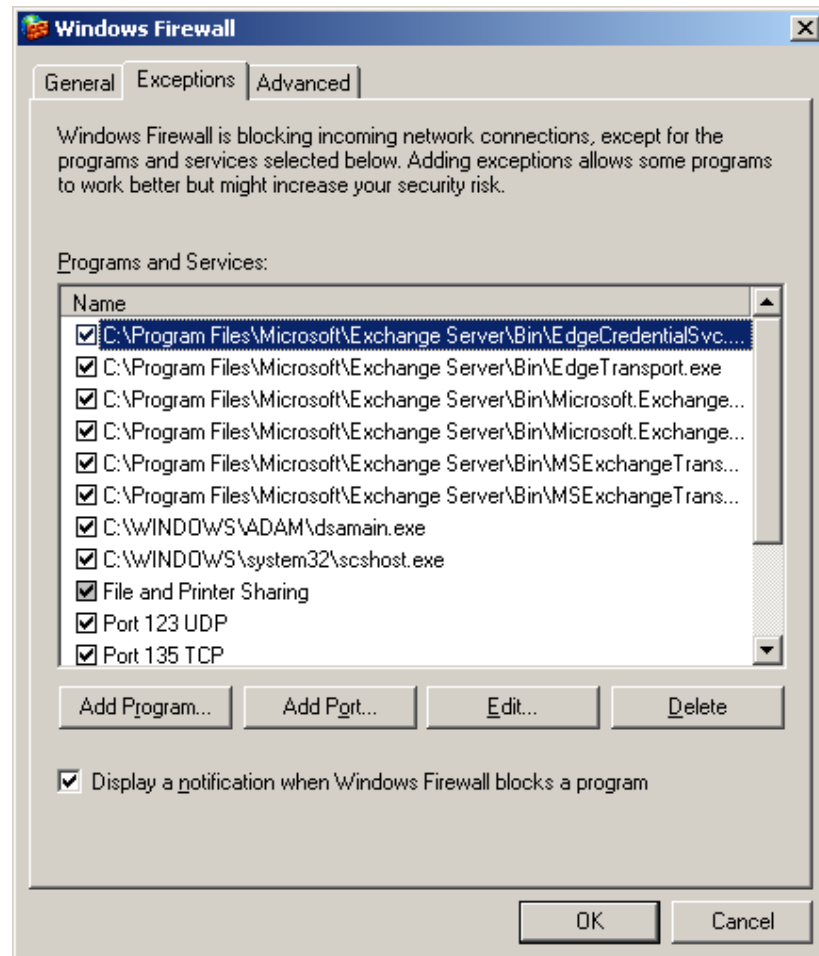
Sau khi hoàn tất áp dụng policy, nhấn **Next**.

Nhấn **Finish** để hoàn tất **Security Configuration Wizard**.

4. Xác nhận các thiết lập bảo mật đã được áp dụng

Vào **Start\Control Panel**, nhấn **Windows Firewall**.

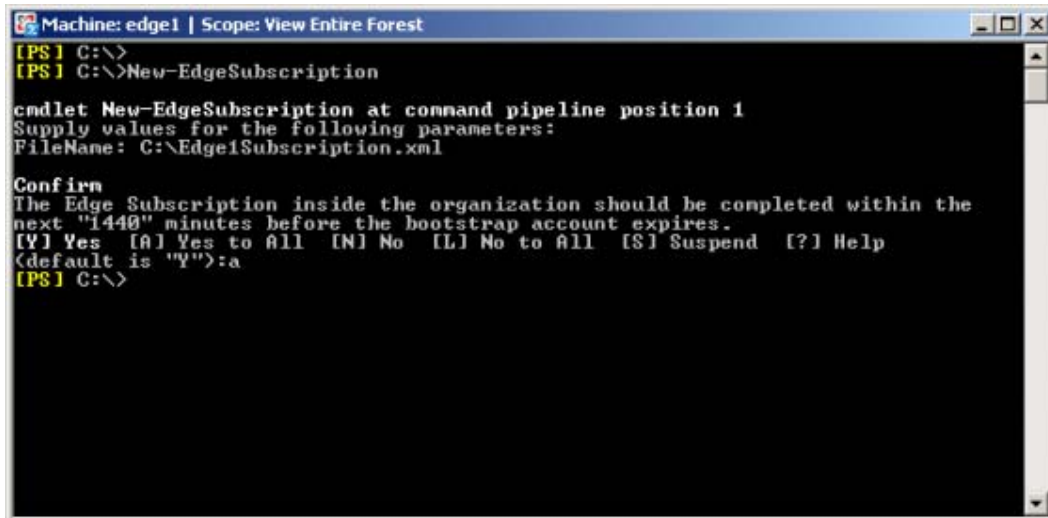
Xác nhận firewall đã được kích hoạt. Trên tab **Exceptions**, xác nhận các tiến trình Exchange-related có xuất hiện. Nhấn **OK**.



Khởi động lại server Edge1.

Cấu hình EdgeSync

1. Xác nhận DNS có thể phân giải được tên Edge Transport Server.
Trên EX01, mở DNS management console từ Administrative Tools.
Mở **Forward Lookup Zones**, nhấn vào **vsiclab.net**.
Xác nhận có entry phân giải **Edge1** thành **192.168.1.222**.
Đóng DNS management console.
2. Tạo file subscription cho Edge1.
Trên Edge1, mở **Exchange Management Shell**, nhập **New-EdgeSubscription**, rồi nhấn ENTER.
Tại dấu nhắc **FileName**, nhập **C:\Edge1subscription.xml** và nhấn ENTER.



```
Machine: edge1 | Scope: View Entire Forest
[PS] C:\>
[PS] C:\>New-EdgeSubscription

cmdlet New-EdgeSubscription at command pipeline position 1
Supply values for the following parameters:
FileName: C:\Edge1Subscription.xml

Confirm
The Edge Subscription inside the organization should be completed within the
next "1440" minutes before the bootstrap account expires.
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help
(default is "Y")>a
[PS] C:\>
```

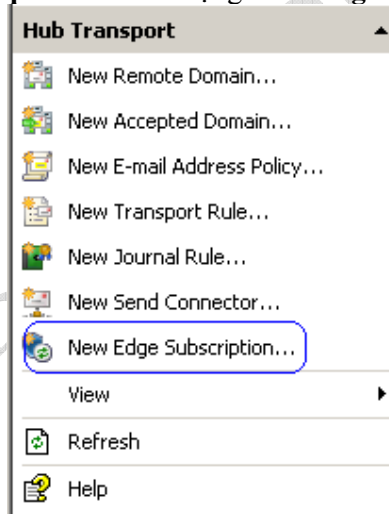
Đóng Exchange Management Shell.

Mở **Windows Explorer**, sao chép file **C:\Edge1subscription.xml** vào **\\EX01\CS**.

3. Cấu hình đồng bộ giữa EX01 và Edge1.

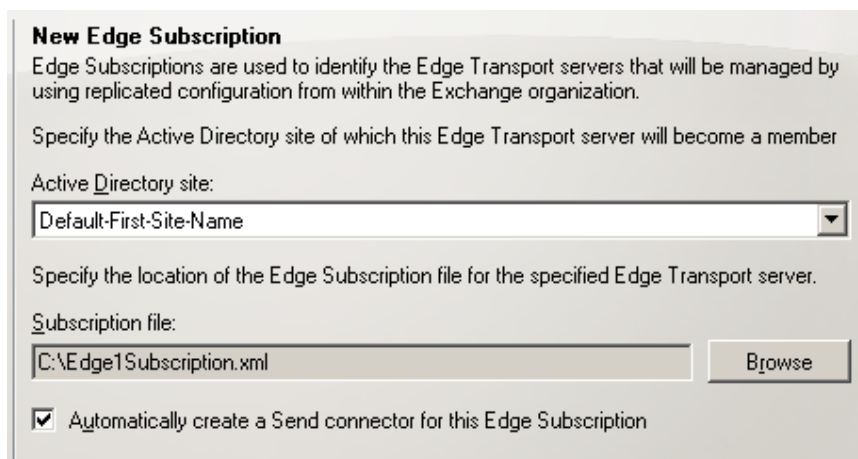
Trên EX01, open the **Exchange Management Console**, mở **Organization Configuration**, and then click **Hub Transport**.

Nhấn **New Edge Subscription** để khởi động **New Edge Subscription wizard**.



Trên **New Edge Subscription** page, click **Browse**.

Trong hộp thoại **Select the Subscription File**, chọn file **C:\Edge1subscription.xml**, và nhấn **Open**.



New Edge Subscription

Edge Subscriptions are used to identify the Edge Transport servers that will be managed by using replicated configuration from within the Exchange organization.

Specify the Active Directory site of which this Edge Transport server will become a member

Active Directory site:

Specify the location of the Edge Subscription file for the specified Edge Transport server.

Subscription file:

☒ Automatically create a Send connector for this Edge Subscription

Trên trang **New Edge Subscription** page, click **New**, and then click **Finish**.

Đóng **Exchange Management Console**.

4. Xác nhận đồng bộ giữa EX01 và Edge1.

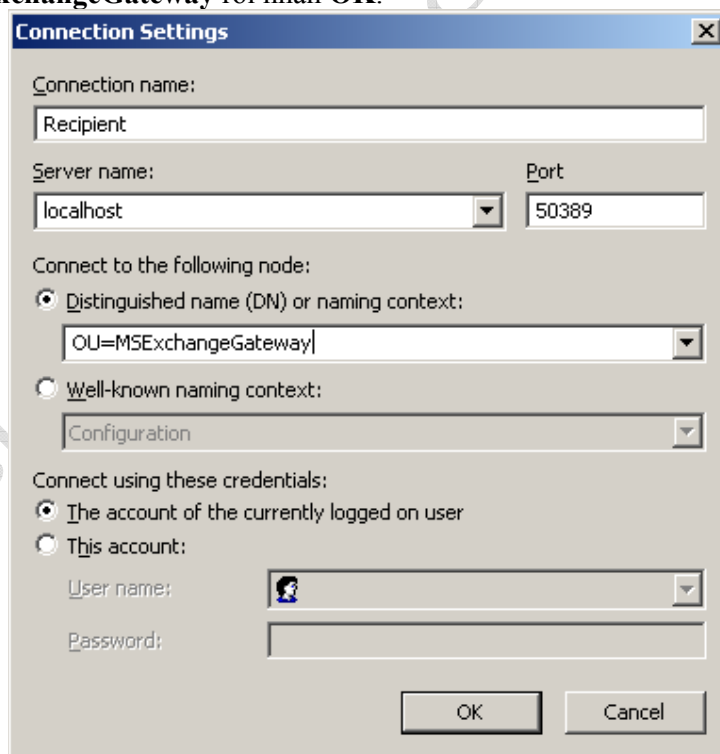
Trên **Start** menu, vào **All Programs\ADAM\ADAM ADSI Edit**.

Trong console tree, nhấn phải vào **ADAM ADSI Edit**, rồi chọn **Connect to**.

Trong hộp thoại **Connection Settings**, trong hộp **Connection name**, nhập **Recipients**

Trong ô **Port**, đổi thành **50389**.

Chọn **Distinguished name (DN) or naming context**, và nhập **OU=MSExchangeGateway** rồi nhấn **OK**.



Connection Settings

Connection name:

Server name: Port:

Connect to the following node:

☒ Distinguished name (DN) or naming context:

☐ Well-known naming context:

Connect using these credentials:

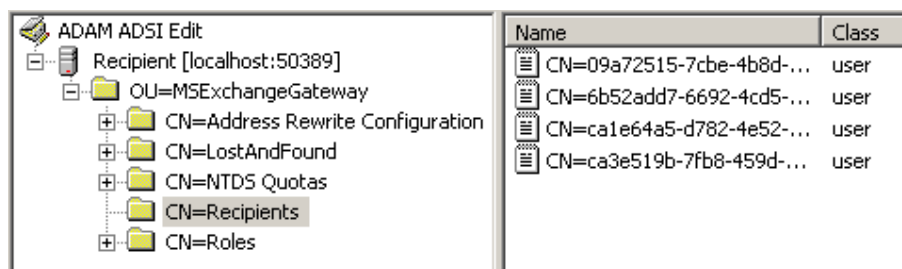
☒ The account of the currently logged on user

☐ This account:
 User name:
 Password:

Mở **Recipients [localhost:50389]**, rồi mở **OU=MSExchangeGateway**. Xác nhận **CN=Recipients** container đã được tạo dưới **OU=MSExchangeGateway**.

Chú ý: Việc đồng bộ có thể mất vài phút, nếu thấy quá lâu có thể dùng **Start-EdgeSynchronization** cmdlet để kích hoạt tiến trình đồng bộ.

Nhấn **CN=Recipients**, xác nhận các user trong domain vsiclab.net đã xuất hiện.



Đóng ADAM-adsiedit.

Bài tập 2 Cấu hình Domain Security

Công việc chính của bài tập này bao gồm:

Cấu hình các SMTP connector trên EX01 server với một certificate dùng chứng thực TLS và mã hóa. Các connector này sẽ chỉ dùng cho kết nối với spamking.com.

Cấu hình danh sách Outbound and Inbound domain security.

Chuẩn bị

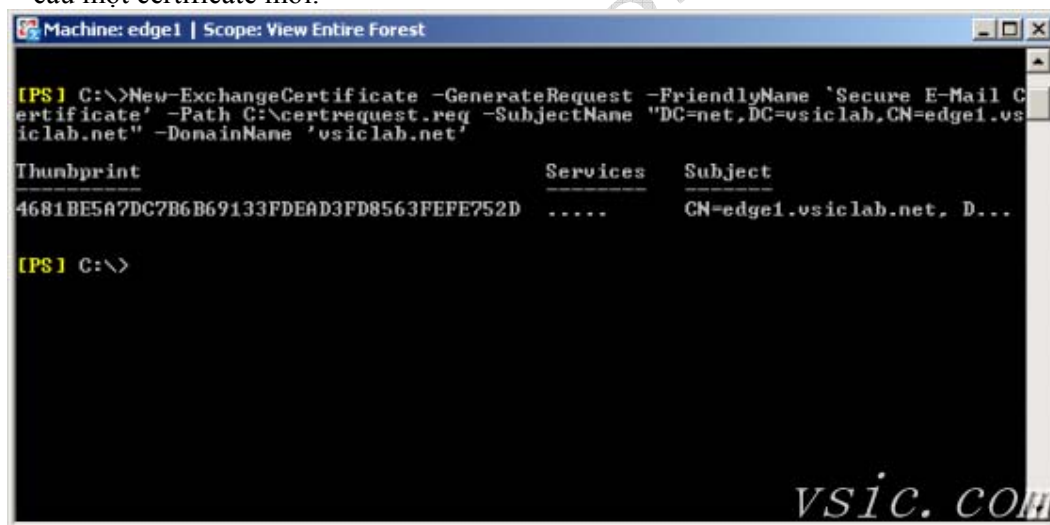
Bài thực hành này cần 2 server

EX01: DNS, DC, Standalone Root CA, Exchange 2007 (Mailbox Server, Client Access, Hub Transport), địa chỉ IP 192.168.1.220.

Edge1: Exchange 2007 (Edge Transport), địa chỉ IP 192.168.1.222.

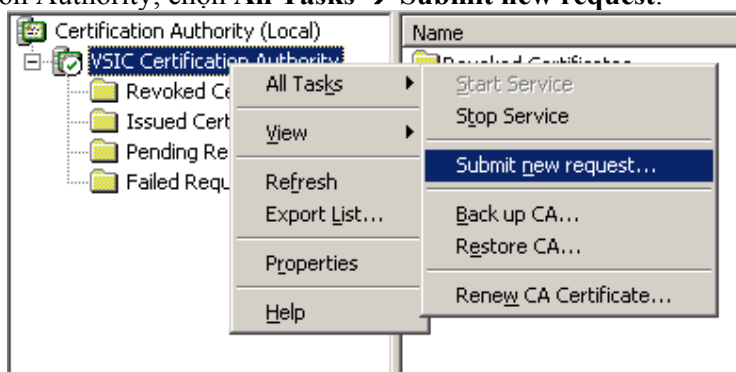
1. Yêu cầu và cài đặt một certificate từ CA.

Trên Edge1, trong **Exchange Management Shell**, dùng lệnh **New-ExchangeCertificate -GenerateRequest -FriendlyName 'Secure E-Mail Certificate' -Path C:\certrequest.req -SubjectName "DC=net,DC=vsiclab,CN=edge1.vsiclab.net" -DomainName 'vsiclab.net'** để yêu cầu một certificate mới.



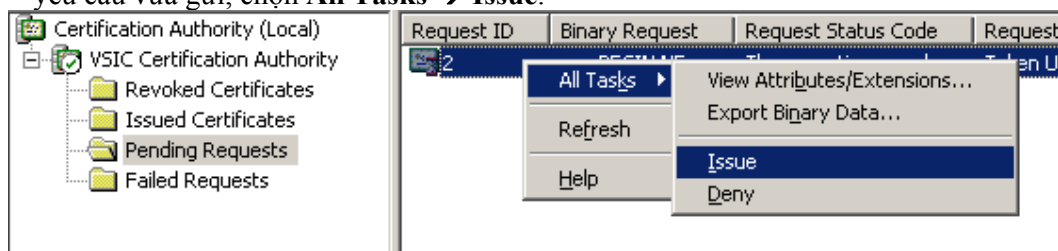
Sao chép file yêu cầu certificate **certrequest.req** đến **\\EX01\c\$**.

Trên EX01, trong Certification Authority MMC snap-in, nhấn phải vào VSIC Certification Authority, chọn **All Tasks** → **Submit new request**.



Chọn file yêu cầu certificate C:\certrequest.req trong hộp thoại **Open Request File**, rồi nhấn **Open**.

Trong Certification Authority MMC snap-in, vào **Pending Requests**, nhấn phải vào yêu cầu vừa gửi, chọn **All Tasks → Issue**.

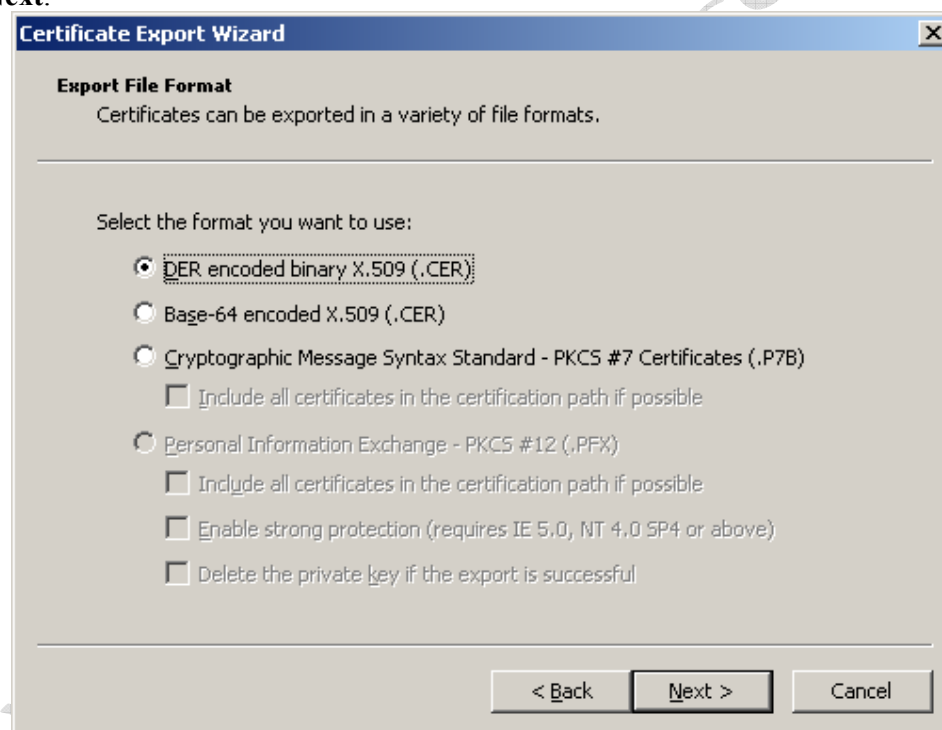


Trong Certification Authority MMC snap-in, vào Issued Certificates, nhấn phải vào certificate vừa cấp phát, chọn **Open**.

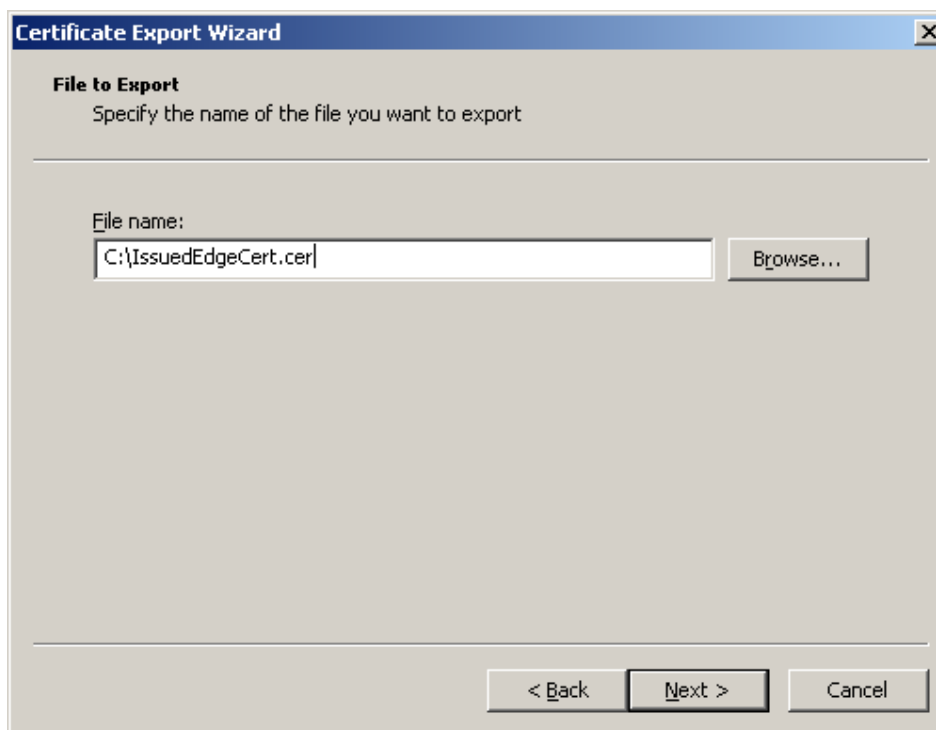
Trong hộp thoại Certificate, vào tab **Details**, nhấn **Copy to File**.

Trên trang Certificate Export Wizard, nhấn **Next**.

Trên trang Export File Format, chọn **DER encoded binary X.509 (.CER)**, rồi nhấn **Next**.



Trên trang Export to File, xác định file tạo ra là **C:\IssuedEdgeCert.cer**, nhấn **Next**, rồi nhấn **Finish** để kết thúc wizard.



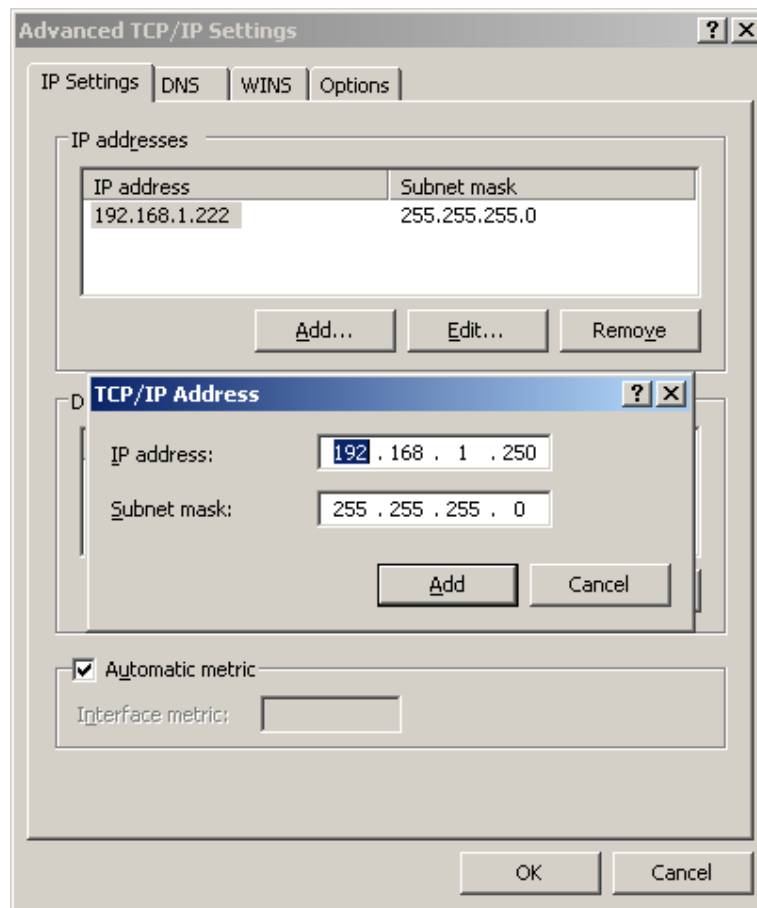
Sao chép file **C:\IssuedEdgeCert.cer** vào **\\Edge1\C\$**.

Trên Edge1, trong **Exchange Management Shell**, dùng lệnh **Import-ExchangeCertificate -Path C:\IssuedEdgeCert.cer / Enable-ExchangeCertificate -Services SMTP** để import certificate.

2. Trên Edge1, bổ sung thêm một địa chỉ IP mới 192.168.1.250 vào Local Area Connection. Địa chỉ IP này sẽ được dành riêng cho kết nối với Spamking.

Trên Edge1, truy cập vào **Local Area Connection properties**, rồi vào **Internet Protocol (TCP/IP) Properties**, nhấn **Advanced**.

Trong hộp thoại **Advanced TCP/IP Settings**, vào tab **IP Settings**, nhấn **Add**, rồi nhập địa chỉ IP **192.168.1.250**, subnet mask **255.255.255.0** vào hộp thoại **TCP/IP Address**.



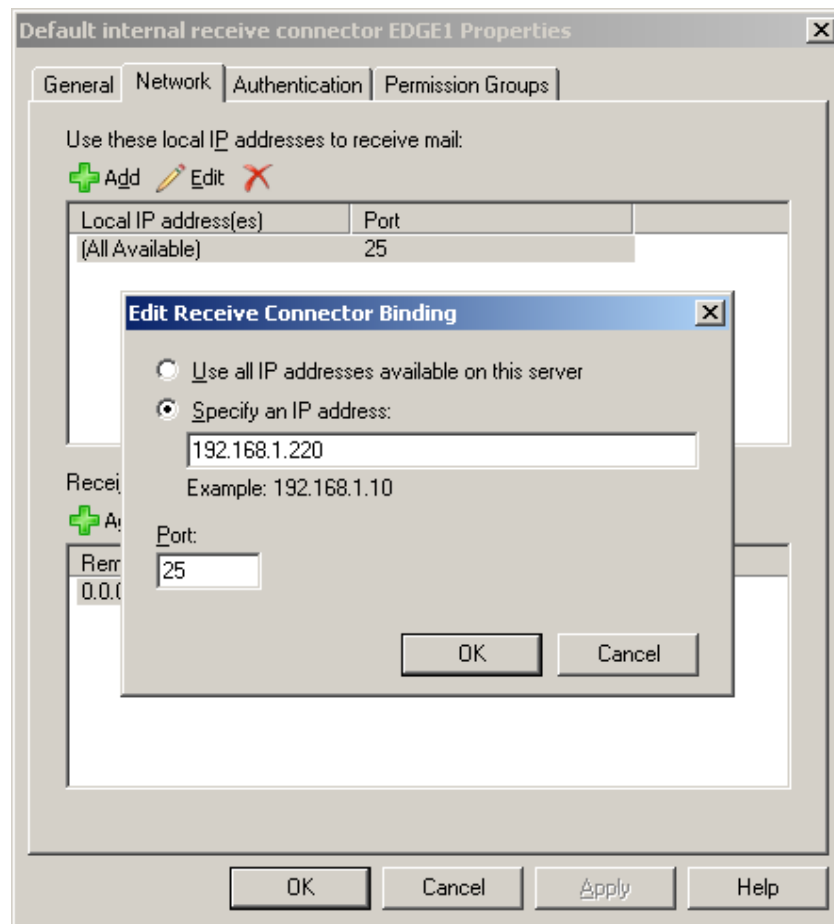
Nhấn **Add**, rồi nhấn **OK** 3 lần để thoát khỏi hộp thoại **Local Area Connection properties**.

3. Trên Edge1, thay đổi cấu hình của SMTP Receive connector mặc định, và tạo một SMTP Receive connector mà sẽ dùng để nhận e-mail từ spamking.com.

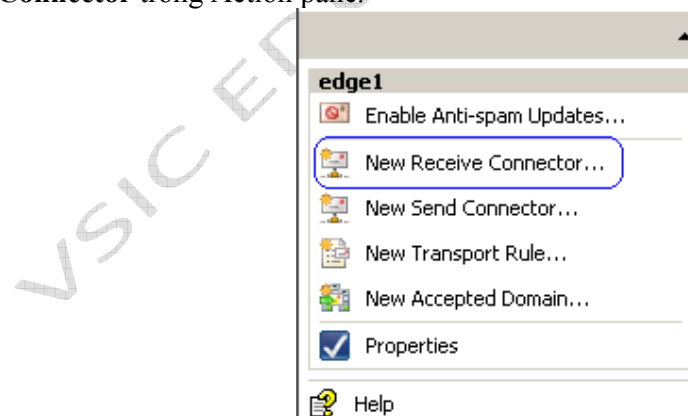
Trên Edge1, trong **Exchange Management Console\Organization Configuration\Edge Transport**, vào tab **Receive connector**, nhấn phải vào **Default internal Receive connector EDGE1** chọn **Properties**.

Trong hộp thoại **Default internal Receive connector EDGE1 Properties**, vào tab **Network**, chọn **(All Available)** tại **Local IP address(es)**, nhấn **Edit**.

Trong hộp thoại **Edit Receive Connector Binding**, chọn **Specify an IP address** và nhập vào địa chỉ IP **192.168.1.220**. Nhấn **OK** 2 lần để hoàn tất.



Trên Edge1, trong **Exchange Management Console\Organization Configuration\Edge Transport**, vào tab **Receive connector**, nhấn **New Receive Connector** trong Action pane.



Trên trang **Introduction**, nhập tên connector là Spamking Receive Connector, nhấn **Next**.

Introduction

This wizard helps you create a new Receive connector on the selected Exchange server. To configure properties not shown in this wizard, in the Exchange Management Console, select the new connector. Then, in the action pane, click Properties.

Name:




Select the intended use for this Receive connector:

Description: Select this option to create a customized connector, which will be used to connect with systems that are not Exchange servers.

Trên trang **Local Network settings**, chọn **(All Available)** tại **Local IP address(es)**, nhấn **Edit**, nhập vào địa chỉ IP **192.168.1.250**. Nhấn **OK** rồi nhấn **Next**.

Local Network settings

Use these local IP addresses to receive mail:

 Add  Edit 

Local IP address(es)	Port
(All Available)	25

Edit Receive Connector Binding

☐ Use all IP addresses available on this server

☒ Specify an IP address:

Example: 192.168.1.10

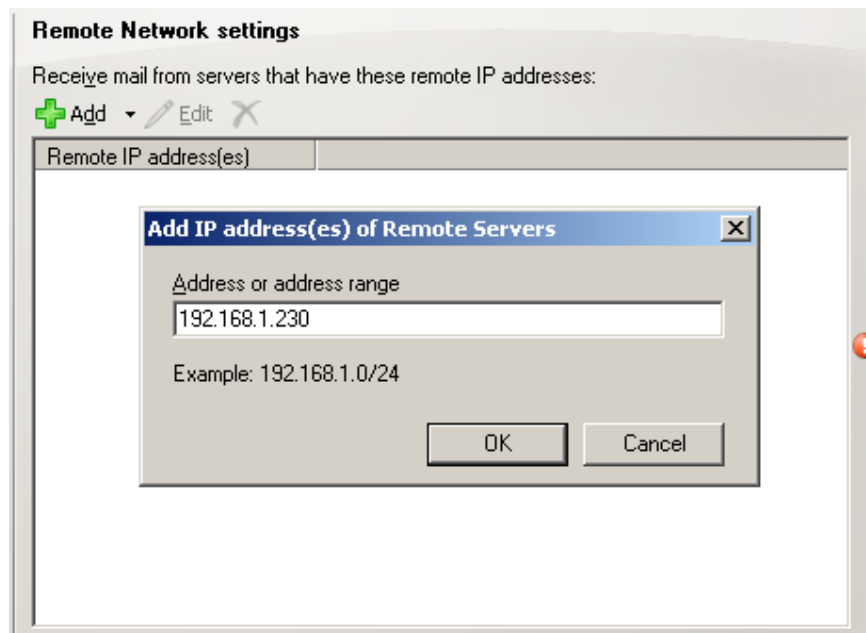
Port:

OK Cancel

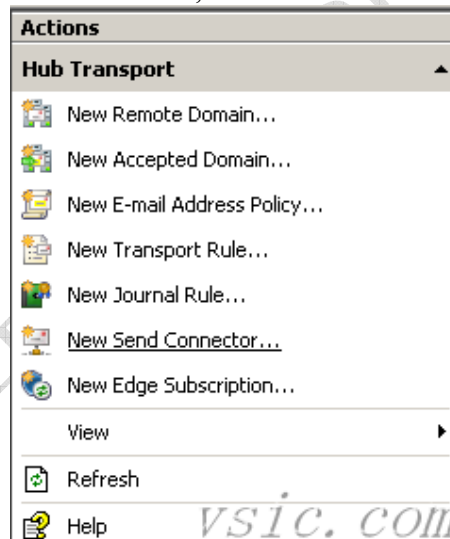
Specify the FQDN this connector will provide in response to HELO or EHLO:

(Example: mail.contoso.com)

Trên trang **Local Network settings**, xóa entry **0.0.0.0-255.255.255.255** tại **Remote IP address(es)**, rồi nhấn **Add**, nhập vào địa chỉ IP **192.168.1.230**. Nhấn **OK** rồi nhấn **Next**.



4. Trên EX01, tạo một SMTP Send connector mà sẽ dùng để gửi e-mail đến spamking.com.
Trên EX01, vào **Exchange Management Console\Organization Configuration\Hub Transport**, vào tab **Send Connectors**, nhấn **New Send Connector** trong Action pane.



Trong trang Introduction, nhập tên connector là **Spamking Send Connector**, chọn ý định sử dụng là **Partner**, nhấn Next.

Introduction

This wizard helps you create a new SMTP Send connector on the selected Exchange server. To configure properties not shown in this wizard, in the Exchange Management Console, select the new connector. Then, in the action pane, click Properties.

Name:



Select the intended use for this Send connector:

Description: Partner Send connectors are used to send e-mail to partner domains. This connector will be configured to only allow connections to servers that authenticate with Transport Layer Security (TLS) certificates for SMTP domains that are included in the list of domain-secured domains. You can add domains to this list by using the `TLSSendDomainSecureList` parameter in the `Set-TransportConfig` command.

Trong trang **Address space**, nhấn **Add** và nhập **spamking.com** vào hộp thoại **Add address space**, nhấn **OK** rồi nhấn **Next**.

Address space

Specify the address space(s) to which this connector will route mail.

 Add 



Domain	Type
<div style="border: 1px solid black; padding: 5px; margin: 10px auto; width: 300px;"> <p>Add Address Space</p> <p>Domain: <input type="text" value="spamking.com"/></p> <p><input checked="" type="checkbox"/> Include all subdomains</p> <p>OK Cancel</p> </div>	

Trên trang **Network Settings**, giữ nguyên thiết lập mặc định, nhấn **Next**.

Trên trang **Source Server**, thêm server Edge1 và xoá các server khác nếu có, nhấn **Next**.

Source Server

Associate this connector with the following Hub Transport servers. Alternatively, you can add Edge Subscriptions to this list.

 Add... 

Name	Site	Role
EDGE1	Default-First-Site-Name	Edge Transport

Nhấn **New** ở trang **Connector** và nhấn **Finish** ở trang **Complete** để kết thúc.

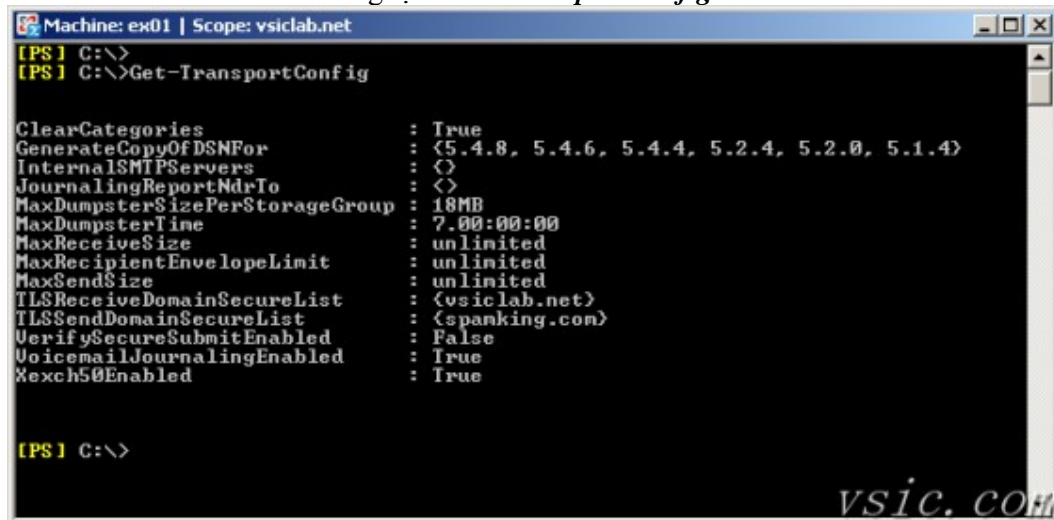
Trên EX01, trong **Exchange Management Shell**, buộc tiến trình **EdgeSync** chạy ngay lập tức bằng lệnh **Start-EdgeSynchronization**.

- Trên EX01, cấu hình danh sách outbound and inbound domain security.

Trên EX01, trong **Exchange Management Shell**, bổ sung spamking.com vào danh sách send domain bằng lệnh sau: **Set-TransportConfig -TLSSendDomainSecureList spamking.com**.

Trên EX01, trong **Exchange Management Shell**, bổ sung vsiclab.net vào danh sách receive domain bằng lệnh sau: **Set-TransportConfig -TLSReceiveDomainSecureList vsiclab.net**.

Kiểm tra các cấu hình bằng lệnh **Get-TransportConfig**.



```
Machine: ex01 | Scope: vsiclab.net
[PS] C:\>
[PS] C:\>Get-TransportConfig

ClearCategories                : True
GenerateCopyOfDSNFor          : <5.4.8, 5.4.6, 5.4.4, 5.2.4, 5.2.0, 5.1.4>
InternalSMTPServers            : <>
JournalingReportNdrTo         : <>
MaxDumpsterSizePerStorageGroup : 18MB
MaxDumpsterTime               : 7.00:00:00
MaxReceiveSize                : unlimited
MaxRecipientEnvelopeLimit     : unlimited
MaxSendSize                   : unlimited
TLSReceiveDomainSecureList    : <vsiclab.net>
TLSSendDomainSecureList       : <spanking.com>
VerifySecureSubmitEnabled     : False
VoicemailJournalingEnabled    : True
Xexch50Enabled                : True

[PS] C:\>
```

Module 3 Implementing Messaging Policies

Bài tập 1 Cấu hình Messaging Records Management

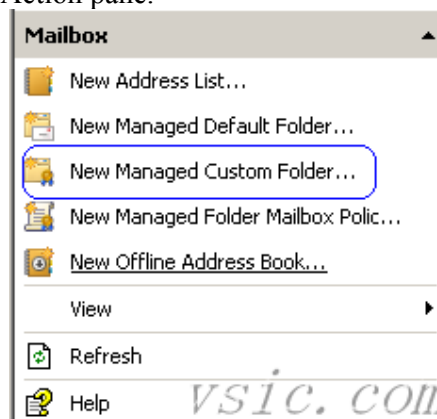
Trong bài tập này, bạn sẽ tạo một thư mục managed custom folder và cấu hình thiết lập managed content. Sau đó, bạn sẽ tạo chính sách managed content policies và gán chính sách này cho các user theo yêu cầu.

Chuẩn bị

Trên EX01, và **Active Directory Users and Computers**, tạo một OU **Gryffindor**.

1. Tạo một thư mục managed custom mailbox folder named **Gryffindor Confidential**.

Trên EX01, vào **Exchange Management Console\Organization Configuration\Mailbox**, vào tab **Managed Custom Folders**, nhấn **New Managed Custom Folder** trong Action pane.



Trong trang **New Managed Custom Folder**, nhập tên **Gryffindor Confidential**, chú thích **All confidential items related to Gryffindor should be posted here. Messages in this folder are valid for 180 days** và chọn **Do not allow users to minimize the comment in Outlook**, rồi nhấn **New**.

New Managed Custom Folder

Managed custom folders are mailbox folders with settings that control the content within the folder.

Name:
Gryffindor Confidential

Display the following name when the folder is viewed in Office Outlook:
Gryffindor Confidential

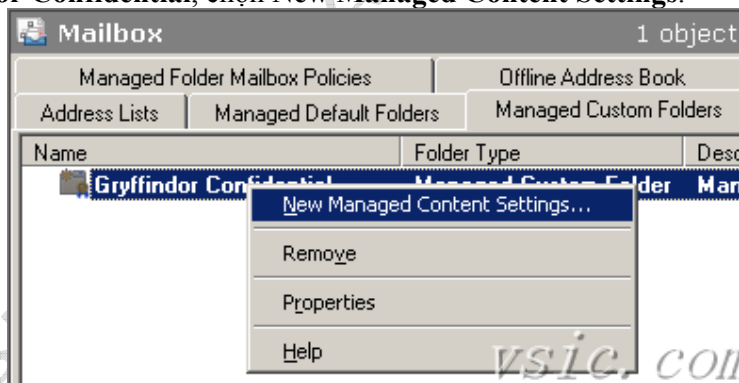
☐ Storage limit (KB) for this folder and its subfolders:

Display the following comment when the folder is viewed in Outlook:
All confidential items related to Gryffindor should be posted here. Messages in this folder are valid for 180 days

☒ Do not allow users to minimize this comment in Outlook.

2. Cấu hình thiết lập nội dung cho thư mục Finance Confidential folder để tất cả các message sẽ được giữ lại trong 180 ngày, sau đó message sẽ được đánh dấu hết hạn trong Outlook.

Trên EX01, vào **Exchange Management Console\Organization Configuration\Mailbox**, vào tab **Managed Custom Folders**, nhấn phải vào **Gryffindor Confidential**, chọn **New Managed Content Settings**.



Trong trang Introduction, nhập tên **Gryffindor Confidential Content Settings**, kiểu message **All Mailbox Content**. Cấu hình để message được giữ lại sau **180** kể từ khi chuyển vào thư mục này. Sau khi hết thời hạn duy trì, message sẽ được đánh dấu **Past Retention Limit** trong Outlook, rồi nhấn **Next**.

Introduction
Managed content settings allow you to control the lifespan of items of the specified message type.

Name of the managed content settings to be displayed in the Exchange Management Console:

Message type:

☒ Length of retention period (days):

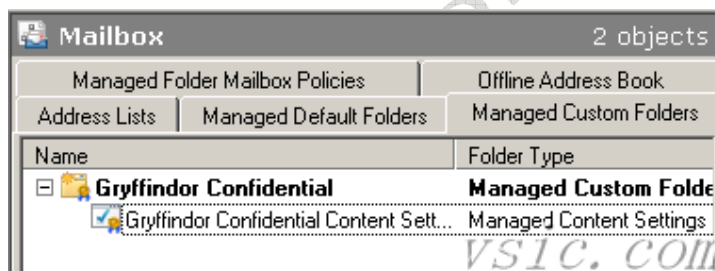
Retention period starts:

Action to take at the end of the retention period:

Move to the following managed custom folder:

Note: The target managed custom folder must already exist. Managed custom folders are created by using the New Managed Folder wizard.

Trong trang **Jounaling**, giữ nguyên mọi thiết lập, nhấn **Next**, nhấn **New** rồi **Finish** để kết thúc.



3. Cấu hình thiết lập nội dung cho tất cả các thư mục mailbox khác để các message sẽ bị xóa bỏ sau 90 ngày.

Trên EX01, vào **Exchange Management Console\Organization Configuration\Mailbox**, vào tab **Managed Default Folders**, nhấn phải vào **Entire Mailbox**, chọn **New Managed Content Settings**.

Trong trang Introduction, nhập tên **Mailbox Content Settings**, kiểu message **All Mailbox Content**. Cấu hình để message được giữ lại sau **90** kể từ khi message được giao. Sau khi hết thời hạn duy trì, message sẽ được xóa bỏ và cho phép phục hồi., rồi nhấn **Next**.

Introduction
Managed content settings allow you to control the lifespan of items of the specified message type.

Name of the managed content settings to be displayed in the Exchange Management Console:

Mailbox Content Settings

Message type:

All Mailbox Content

☒ Length of retention period (days): 90

Retention period starts:

When delivered, end date for calendar and recurring tasks

Action to take at the end of the retention period:

Delete and Allow Recovery

Move to the following managed custom folder:

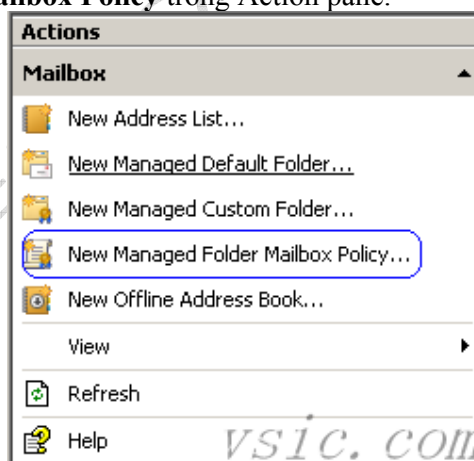
Browse...

Note: The target managed custom folder must already exist. Managed custom folders are created by using the New Managed Folder wizard.

Trong trang **Journaling**, giữ nguyên mọi thiết lập, nhấn **Next**, nhấn **New** rồi **Finish** để kết thúc.

4. Cấu hình chính sách managed folder mailbox mà sẽ áp dụng cho tất cả user. to all users.

Trên EX01, vào **Exchange Management Console\Organization Configuration\Mailbox**, vào tab **Managed Folders Mailbox Policy**, nhấn **New Managed Folder Mailbox Policy** trong Action pane.



Trong trang **New Mailbox Policy**, nhập tên **Default Policy – All Users**. Nhấn **Add** rồi chọn **Entire Mailbox**, nhấn **OK** rồi nhấn **New** và nhấn **Finish** để kết thúc.

New Mailbox Policy

A managed folder mailbox policy groups together a set of managed folders so that you can add multiple folders to a user mailbox in a single step.

Managed folder mailbox policy name:

Mailbox Content Settings

Specify the managed folders that you want to link to this policy:

+ Add... X

Folder	Description	Folder Type
Entire Mailbox	Managed Default Folder	All other folders in the mail

Vào Exchange Management Console, sử dụng lệnh **Get-Mailbox | Set-Mailbox – ManagedFolderMailboxPolicy ‘Default Policy – All Users’** để gán policy cho tất cả user.

5. Cấu hình chính sách managed folder mailbox áp dụng cho Gryffindor.

Trên EX01, vào **Exchange Management Console\Organization**

Configuration\Mailbox, vào tab **Managed Folders Mailbox Policy**, nhấn **New Managed Folders Mailbox Policy** trong Action pane.

Trong trang **New Mailbox Policy**, nhập tên **Griffindor Policy**. Nhấn **Add** rồi chọn **Entire Mailbox** và **Gryffindor Confidential**, nhấn **OK** rồi nhấn **New** và nhấn **Finish** để kết thúc.

New Mailbox Policy

A managed folder mailbox policy groups together a set of managed folders so that you can add multiple folders to a user mailbox in a single step.

Managed folder mailbox policy name:

Griffindor Policy

Specify the managed folders that you want to link to this policy:

+ Add... X

Folder	Description	Folder Type
Entire Mailbox	Managed Default Folder	All other folders in the mail
Gryffindor Confidential	Managed Folder	Managed Custom Folder

Vào Exchange Management Console, sử dụng lệnh `Get-Mailbox | where-object $_.distinguishedname -like '*ou=Gryffindor,dc=vsiclab,dc=net'}` | `Set-Mailbox -ManagedFolderMailboxPolicy 'Gryffindor Policy'` để gán policy cho tất cả user trong OU Gryffindor.

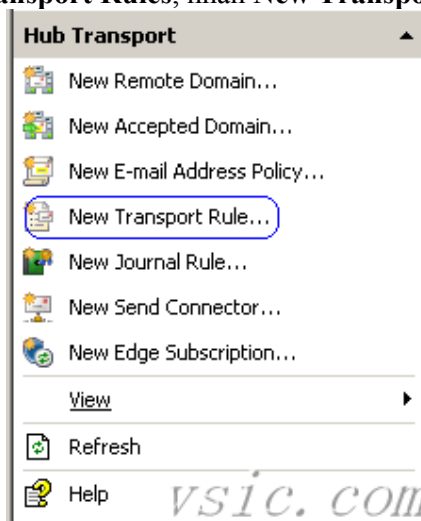
Bài tập 2 Cấu hình luật Transport and Journaling

Trong bài tập này, bạn sẽ cấu hình transport and journaling rule theo yêu cầu của công ty.

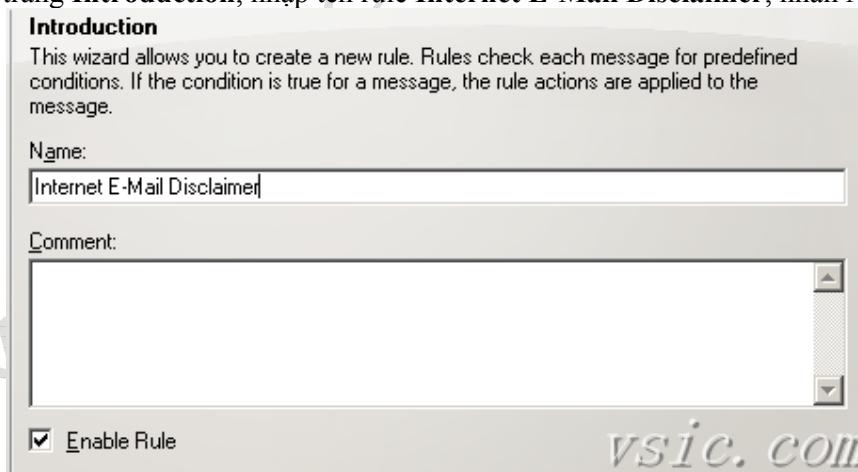
Chuẩn bị

Tạo một distribution group tên Gryffindor với các thành viên là Harry, Ronald.

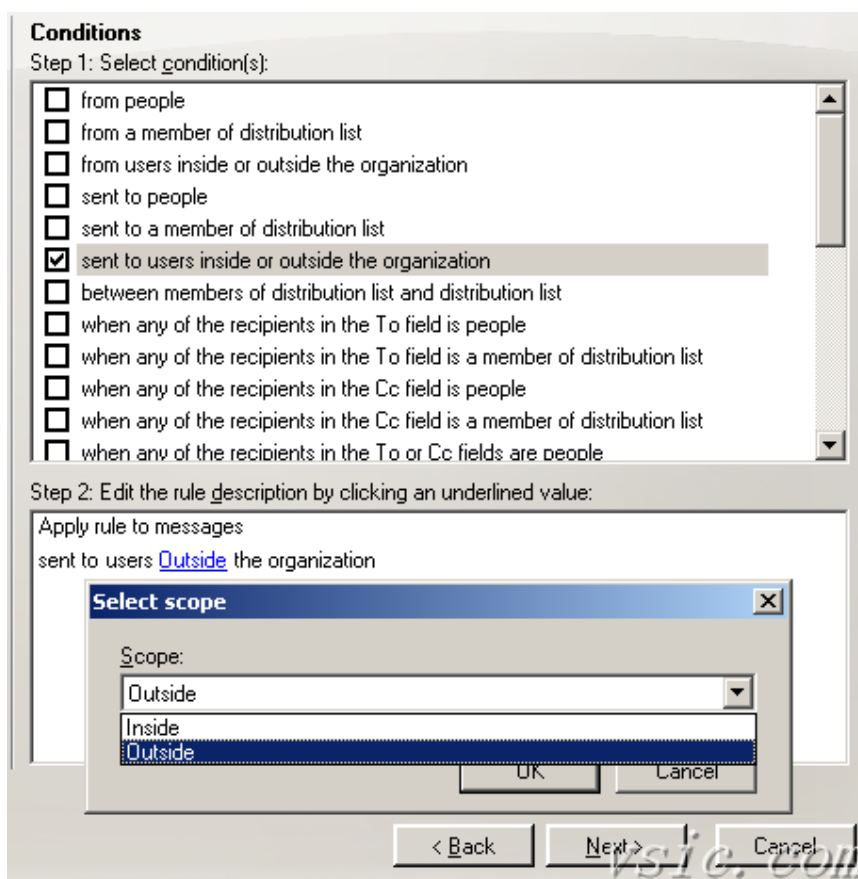
1. Tạo một transport rule để bổ sung một disclaimer vào tất cả các message gửi qua Internet.
Trên EX01, vào **Exchange Management Console\Organization Configuration\Hub Transport**, vào tab **Transport Rules**, nhấn **New Transport Rule Action** pane.



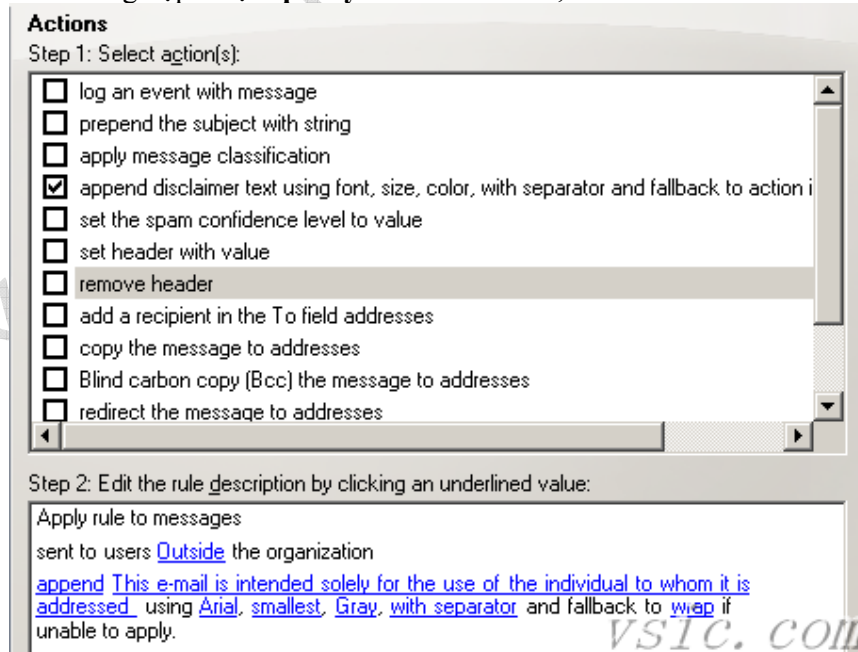
Trên trang **Introduction**, nhập tên rule **Internet E-Mail Disclaimer**, nhấn **Next**.



Trên trang **Conditions**, chọn **Sent to users inside or outside the organization**, nhấn **Next** và **Inside**, chọn scope **Outside** trong hộp thoại **Select scope**, nhấn **OK** rồi nhấn **Next**.



Trên trang **Actions**, chọn **append disclaimer text ...**, nhấn vào **disclaimer text**, nhập vào **This e-mail is intended solely for the use of the individual to whom it is addressed** trong hộp thoại **Specify disclaimer text**, nhấn **OK** rồi nhấn **Next**.



Trên trang **Exceptions**, nhấn **Next**, rồi nhấn **New**, nhấn **Finish** để kết thúc.

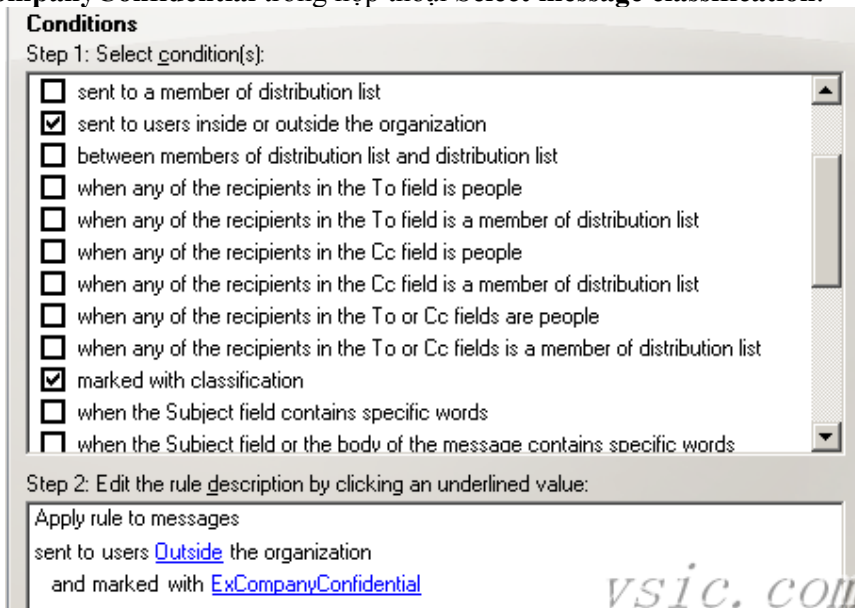
2. Tạo một transport rule để chặn tất cả message thuộc loại Company Confidential gửi ra Internet.

Trên EX01, vào **Exchange Management Console\Organization Configuration\Hub Transport**, vào tab **Transport Rules**, nhấn **New Transport Rule** Action pane.

Trên trang **Introduction**, nhập tên rule **Company Confidential Rule**, nhấn **Next**.

Trên trang **Conditions**, chọn **Sent to users inside or outside the organization**, nhấn và **Inside**, chọn scope **Outside** trong hộp thoại **Select scope**, nhấn **OK** rồi nhấn **Next**. Chọn **Marked with classification**, nhấn vào classification, chọn

ExCompanyConfidential trong hộp thoại **Select message classification**.



Conditions

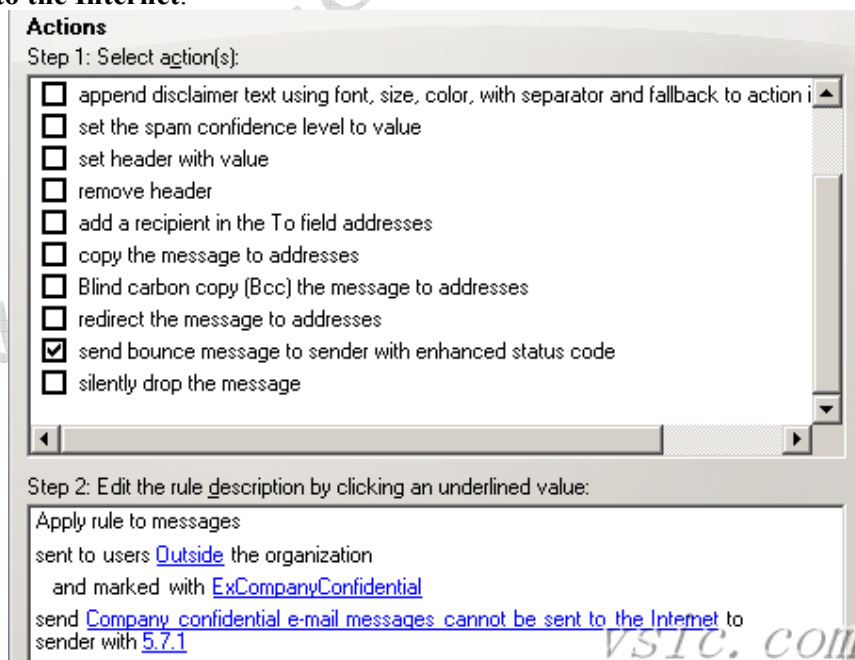
Step 1: Select condition(s):

- ☐ sent to a member of distribution list
- ☒ sent to users inside or outside the organization
- ☐ between members of distribution list and distribution list
- ☐ when any of the recipients in the To field is people
- ☐ when any of the recipients in the To field is a member of distribution list
- ☐ when any of the recipients in the Cc field is people
- ☐ when any of the recipients in the Cc field is a member of distribution list
- ☐ when any of the recipients in the To or Cc fields are people
- ☐ when any of the recipients in the To or Cc fields is a member of distribution list
- ☒ marked with classification
- ☐ when the Subject field contains specific words
- ☐ when the Subject field or the body of the message contains specific words

Step 2: Edit the rule description by clicking an underlined value:

Apply rule to messages
sent to users Outside the organization
and marked with ExCompanyConfidential

Trên trang **Actions**, chọn **send bounce message to sender with enhanced status code**, sửa message text thành **Company confidential e-mail messages cannot be sent to the Internet**.



Actions

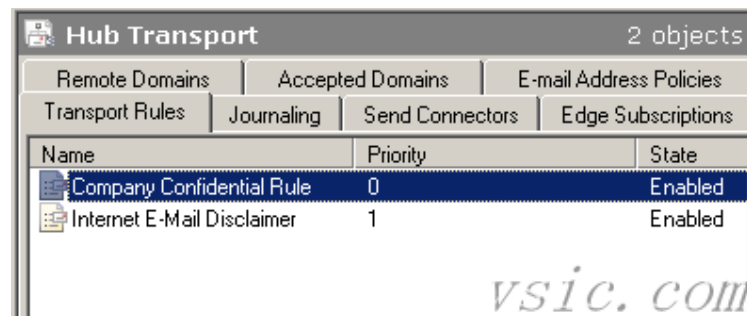
Step 1: Select action(s):

- ☐ append disclaimer text using font, size, color, with separator and fallback to action i
- ☐ set the spam confidence level to value
- ☐ set header with value
- ☐ remove header
- ☐ add a recipient in the To field addresses
- ☐ copy the message to addresses
- ☐ Blind carbon copy (Bcc) the message to addresses
- ☐ redirect the message to addresses
- ☒ send bounce message to sender with enhanced status code
- ☐ silently drop the message

Step 2: Edit the rule description by clicking an underlined value:

Apply rule to messages
sent to users Outside the organization
and marked with ExCompanyConfidential
send Company confidential e-mail messages cannot be sent to the Internet to
sender with 5.7.1

Trên trang **Exceptions**, nhấn **Next**, rồi nhấn **New**, nhấn **Finish** để kết thúc.



3. Tạo một mailbox để journaling messages cho phòng Finance.
the Finance department.

Tạo một recipient với các thuộc tính sau: with the following attributes:

- First name: **Finance Journal Mailbox**
- User Logon name (User Principal Name): **FinanceJournalMailbox**
- Password: <tự đặt>
- Confirm password: <tự đặt>

User Information
Enter the user name and account information.

Organizational unit:
vsiclab.net/Users Browse...

First name: GryffindorJournalMailbox Initials: Last name:

Name: GryffindorJournalMailbox

User logon name (User Principal Name): GryffindorJournalMailbox @vsiclab.net

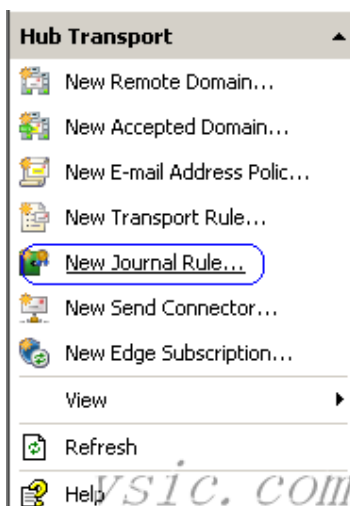
User logon name (pre-Windows 2000): GryffindorJournalMai

Password: Confirm password:

☐ User must change password at next logon

4. Tạo một journal rule mà sẽ lưu một bản sao tất cả các message gửi đi từ user trong Gryffindor.

Trên EX01, vào **Exchange Management Console\Organization Configuration\Hub Transport**, vào tab **Journaling**, nhấn **New Transport Rule** Action pane.



Trên trang New Journal Rule, nhập tên rule **Gryffindor Department Message Journaling**, email address là **GryffindorJournalMailbox**, scope là **Global-all messages**. Chọn **Journal message for recipient**, nhấn **Browse**, chọn **Gryffindor distribution group**. Nhấn **New** rồi nhấn **Finish** để kết thúc.

New Journal Rule
This wizard helps you create a new journal rule. When enabled, the new journal rule is executed on your organization's Hub Transport servers.

Rule name:
Gryffindor Department Message Journaling

Send Journal reports to e-mail address:
GryffindorJournalMailbox Browse...

Scope:
☒ Global - all messages
☐ Internal - internal messages only
☐ External - messages with an external sender or recipient

☒ Journal messages for recipient:
 Gryffindor@vsiclab.net Browse...

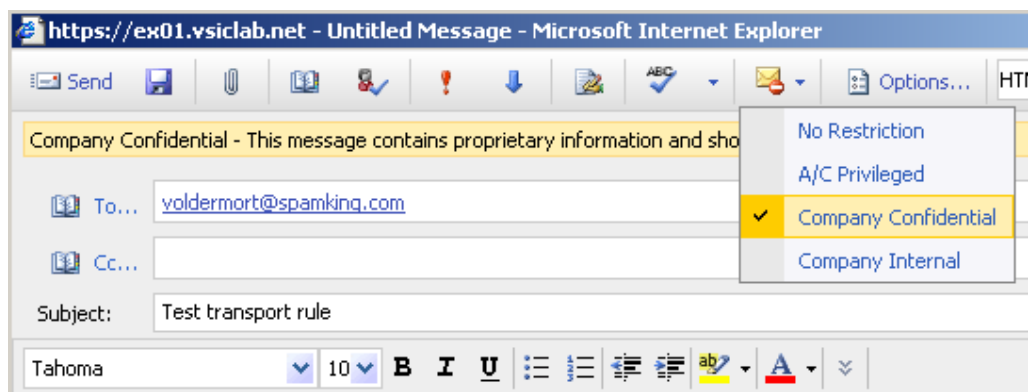
☒ Enable Rule

To use premium journaling, you must have an Exchange Enterprise Client Access License (CAL).

5. Kiểm tra the transport và journaling rules.

Trên EX01, open Internet Explorer and go to **https://ex01/owa**, đăng nhập vào tài khoản Harry và gửi một message đến Voldermort tại spamking.com

Gửi một message khác đến Voldermort đánh dấu message thuộc loại là **Company Confidential**.



Test transport rule

Trên SPAMMER, mở Outlook Express. Xác nhận message thứ nhất gửi từ Harry có disclaimer. Message thứ hai không đến được.

Trên EX01, trong OWA, xác nhận Harry đã nhận được một message từ postmaster báo rằng không thể chuyển giao message đến Voldermort.

Dùng tài khoản Harry gửi một thông điệp mới đến Ronald là thành viên của distribution group Gryffindor.

Đăng nhập vào tài khoản **GryffindorJournalMailbox@vsiclab.net**. Xác nhận journal báo báo có một message được gửi đi từ mailbox của Harry.

Test transport va journaling rule

Microsoft Exchange on behalf of Harry Potter

Sent: Saturday, October 13, 2007 3:03 PM

To: Ronald Weasley

Attachments: Test transport va journaling rule

Sender: harry@vsiclab.net
 Subject: Test transport va
 journaling rule
 Message-Id:
 <C3482050C772FA4E84B7B5785FE437
 To: ronald@vsiclab.net