Network Configuration

In order to properly deploy ExchangeDefender, you need to make several changes on your network. First, you have to change your MX record to point all of your inbound mail to ExchangeDefender. This way ExchangeDefender will stand in front of your mail server and bounce all the dangerous content that is sent to your network. Then, you should change your outbound smarthost to allow us to scan all of your outbound mail*. Finally, enforce IP restrictions so that you can only exchange mail through a trusted connection with ExchangeDefender.

**For users that rely on email for correspondence, outbound network will automatically archive all outbound emails. If you have a business requirement that includes sending out notifications, automated responses, marketing, large distribution lists or other non-correspondance items, we offer outbound-jr high speed relay designed for that specific need.*

MX Record

Please modify your MX record and change it to: **inbound30.exchangedefender.com**

You should not have any other MX records for your domain name (subdomain MX records are OK).

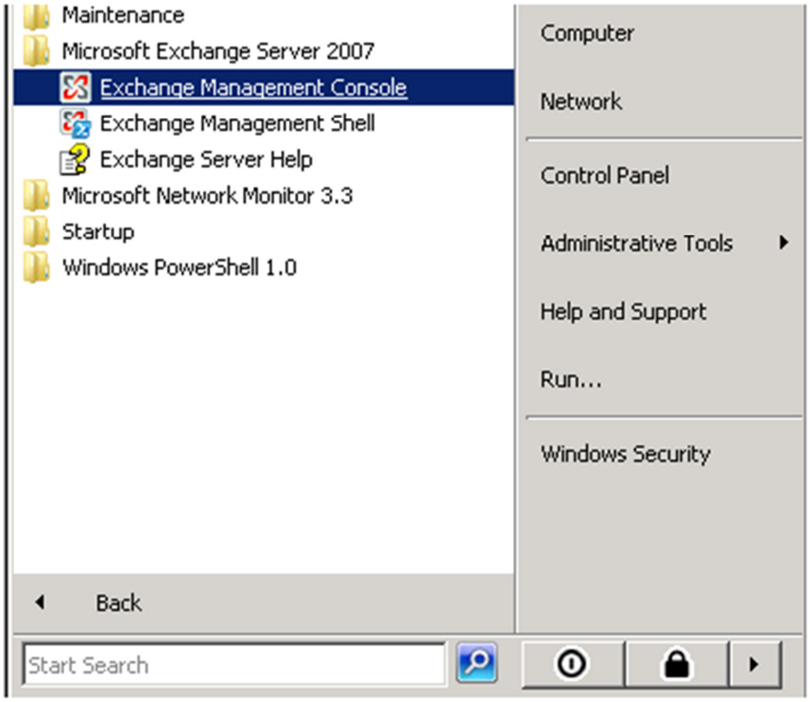
Outbound SmartHost

Please modify your SMTP server to route all outbound mail through the following smarthost: **outbound.exchangedefender.com**

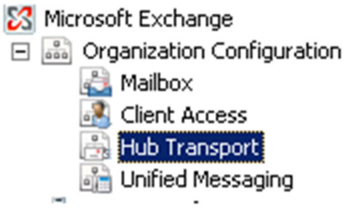
Please follow these instructions to modify the smarthost on Exchange 2003 and 2007:

Exchange 2007

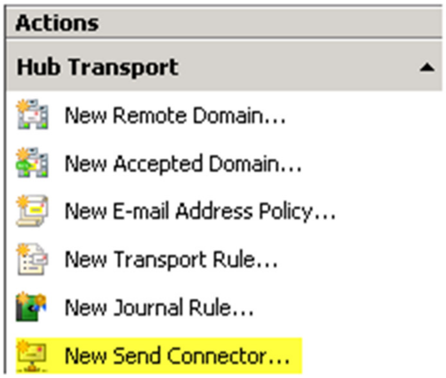
1. Login as the Administrative user to your Exchange 2007 server and open **Exchange Management Console.**



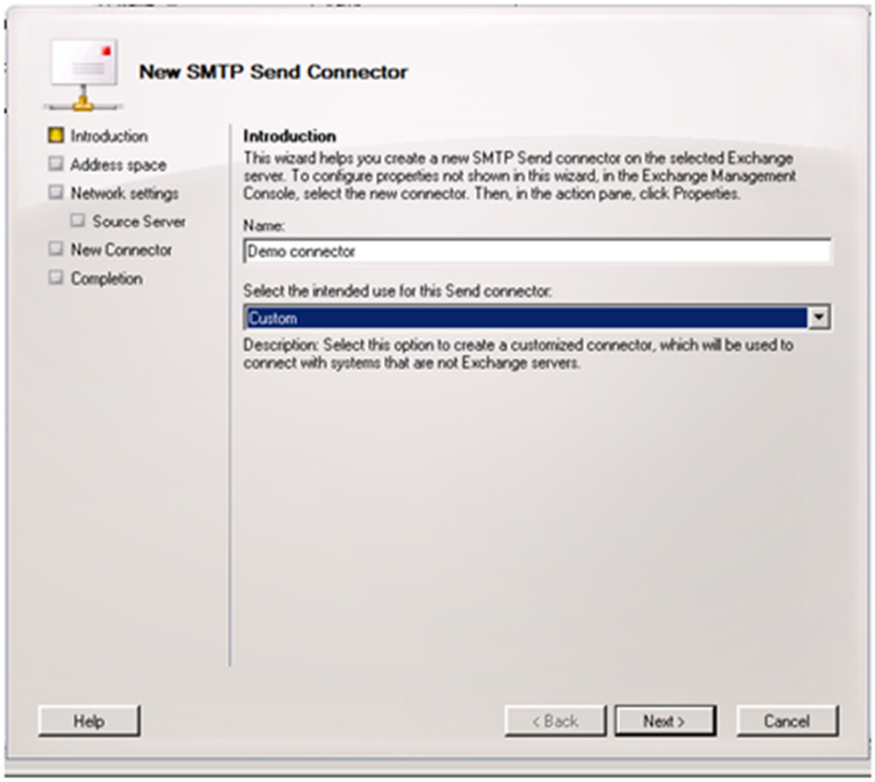
2. Expand *Organizational Configuration*, click **Hub Transport**.



3. On the right hand side under **Actions** click **New Send Connector.**



4. Give the Send Connector a name and select the intended use as *Custom.*



New SMTP Send Connector

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.

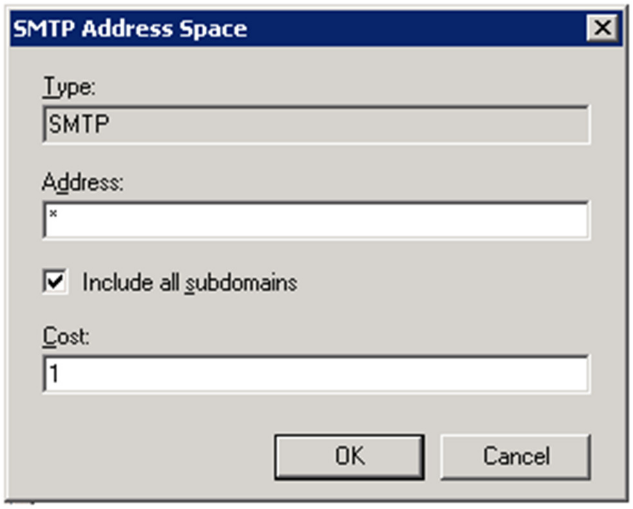
Name: Demo connector

Select the intended use for this Send connector: Custom

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

5. Click the **Add** button on the Address Space screen.

6. Under Address put the recipient domain name, check include all sub-domains and leave the cost as low as possible, click **OK**.



SMTP Address Space

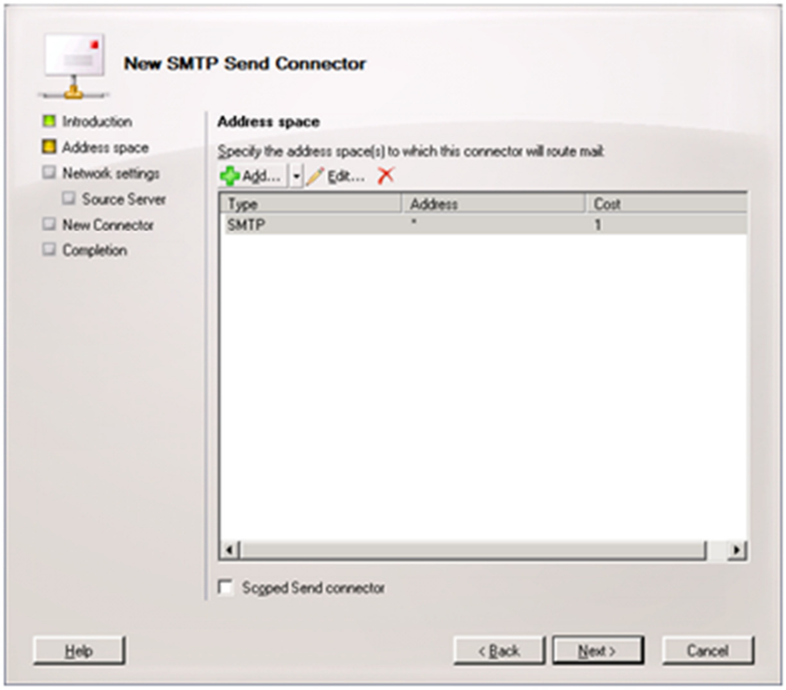
Type: SMTP

Address: *

☑ Include all subdomains

Cost: 1

7. Click **Next**.



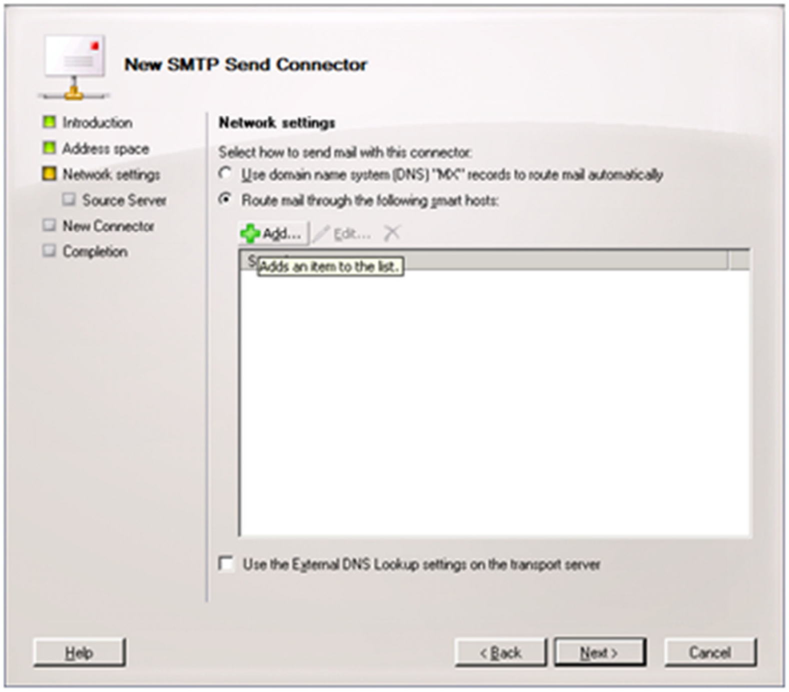
Address space

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

Type	Address	Cost
SMTP	*	1

□ Scoped Send connector

8. Select the radio button to "*Route mail through the follow smart hosts:*" and click **Add**.



Network settings

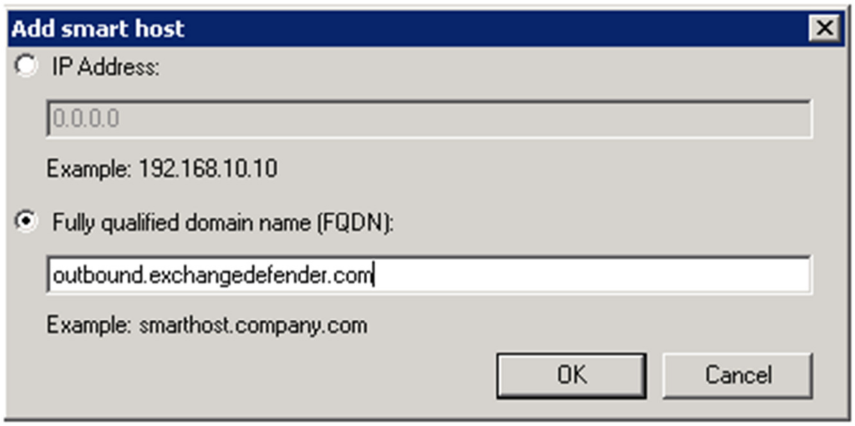
Select how to send mail with this connector:

○ Use domain name system (DNS) "MX" records to route mail automatically

● Route mail through the following smart hosts:

□ Use the External DNS Lookup settings on the transport server

9. Select the radio button to "*Fully qualified domain name (FQDN):*" and enter "*outbound.exchangedefender.com*" and click **OK**.



Add smart host

○ IP Address:

0.0.0.0

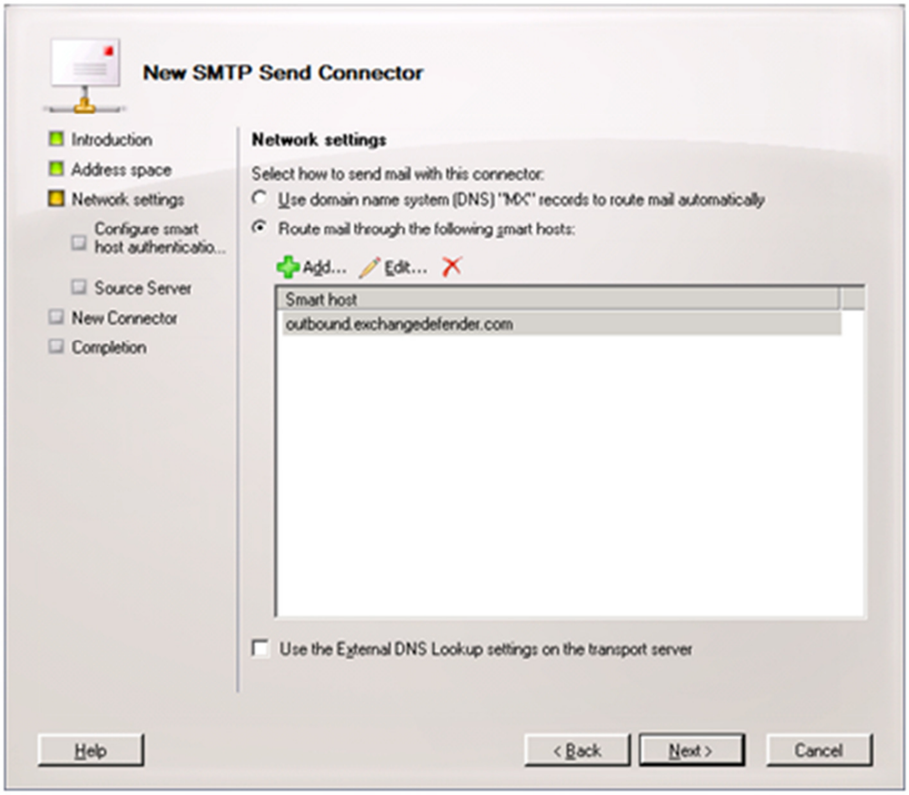
Example: 192.168.10.10

● Fully qualified domain name (FQDN):

outbound.exchangedefender.com

Example: smarthost.company.com

10. At this point, you should be able to see the server you specified listed then click **Next**.



New SMTP Send Connector

Network settings

Select how to send mail with this connector:

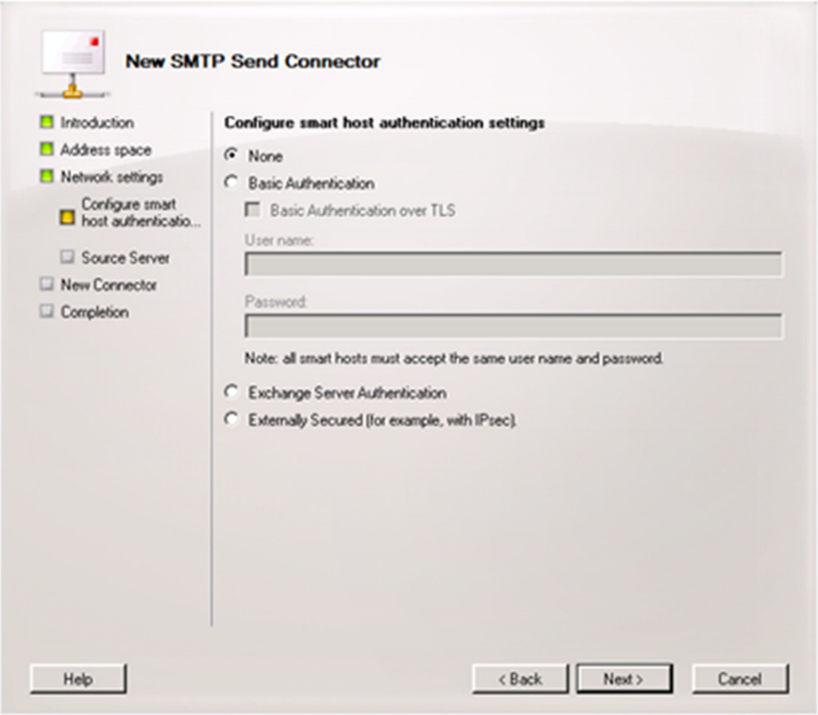
○ Use domain name system (DNS) "MX" records to route mail automatically

● Route mail through the following smart hosts:

Smart host
outbound.exchangedefender.com

□ Use the External DNS Lookup settings on the transport server

11. Since ExchangeDefender uses your server's IP Address to authenticate access, leave the radio button set to Authentication Settings "*None*" and click **Next**.



Configure smart host authentication settings

● None

○ Basic Authentication

□ Basic Authentication over TLS

User name:

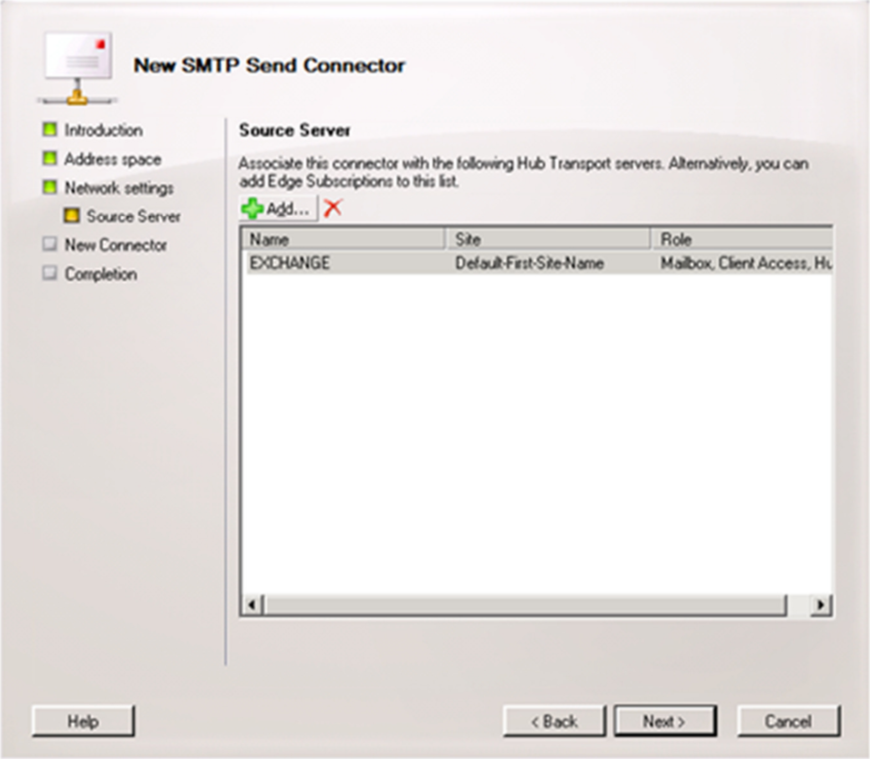
Password:

Note: all smart hosts must accept the same user name and password.

○ Exchange Server Authentication

○ Externally Secured (for example, with IPsec)

12. On the source server screen verify that the exchange server is listed (If not, click Add and find the server) and then click **Next**



Source Server

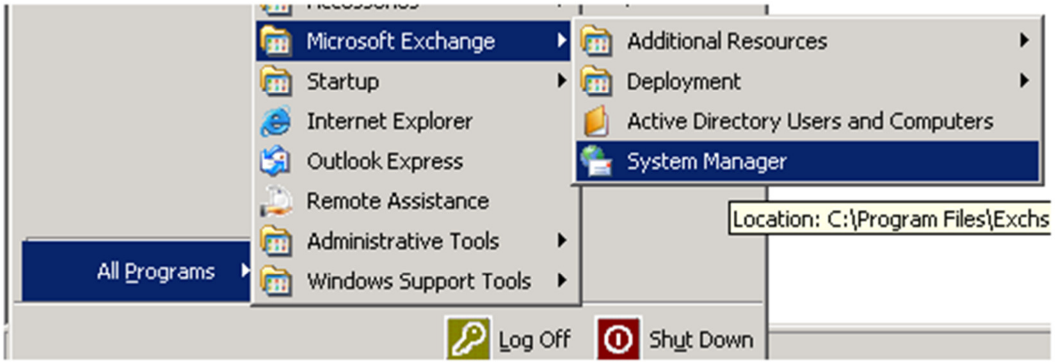
Associate this connector with the following Hub Transport servers. Alternatively, you can add Edge Subscriptions to this list.

Name	Site	Role
EXCHANGE	Default-First-Site-Name	Mailbox, Client Access, Hu

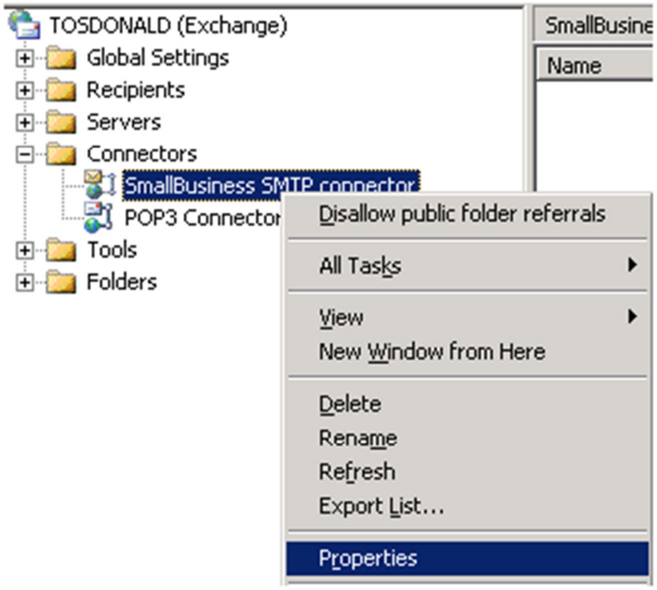
13. On the final screen you will see the commands that will be run to create the send connector. Click **New** and on then **Finish**

Exchange 2003

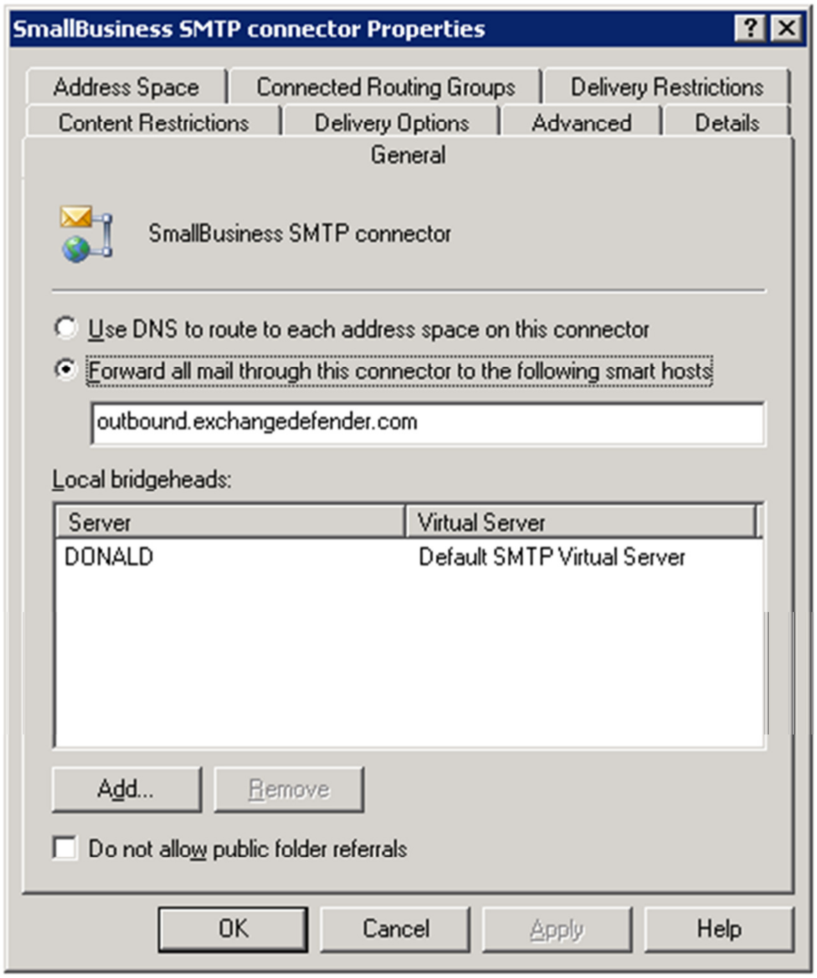
1. Login to your Exchange 2003 server and open *System Manager*.



2. Expand Connectors , right click **SmallBusiness SMTP Connector** (or your active outgoing SMTP connector) and select properties.



3. In the general tab, set the radio option to *Forward all mail through this connector to the following smart hosts* and input *outbound.exchangedefender.com*



SmallBusiness SMTP connector

○ Use DNS to route to each address space on this connector

● Forward all mail through this connector to the following smart hosts

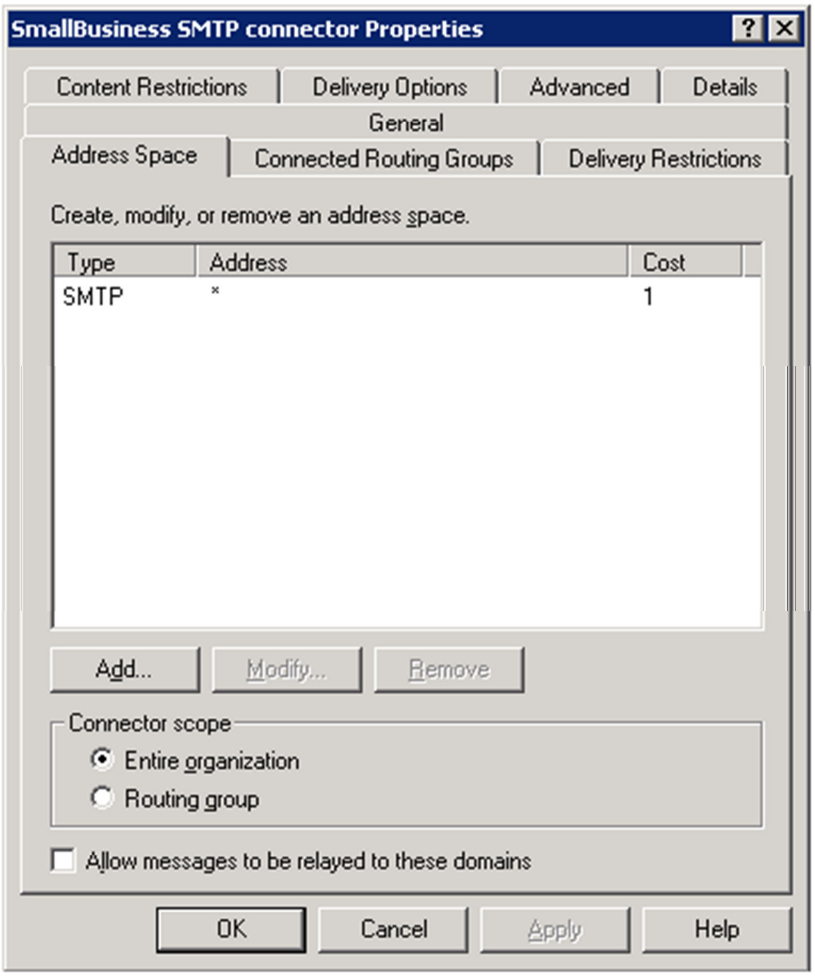
outbound.exchangedefender.com

Local bridgeheads:

Server	Virtual Server
DONALD	Default SMTP Virtual Server

☐ Do not allow public folder referrals

4. Navigate to the *Address Space* tab and ensure there is one entry with the address specified as * and the Cost as 1.



Create, modify, or remove an address space.

Type	Address	Cost
SMTP	*	1

Connector scope

● Entire organization

○ Routing group

□ Allow messages to be relayed to these domains

IP Restrictions

Enforcing IP restrictions is absolutely critical to complete protection of your mail server. Because hackers and spammers can easily bypass cloud services and target your server directly, mail servers protected by ExchangeDefender should accept anonymous SMTP connections only from the ExchangeDefender networks listed below:

65.99.255.0/24
64.182.140.0/24
206.125.40.0/24

You should allow inbound SMTP traffic from the above IP ranges only and deny all other traffic. You should only allow outbound SMTP traffic from your mail server to the ExchangeDefender outbound servers.

Please follow these instructions to enforce IP restrictions on Exchange 2003 and 2007:

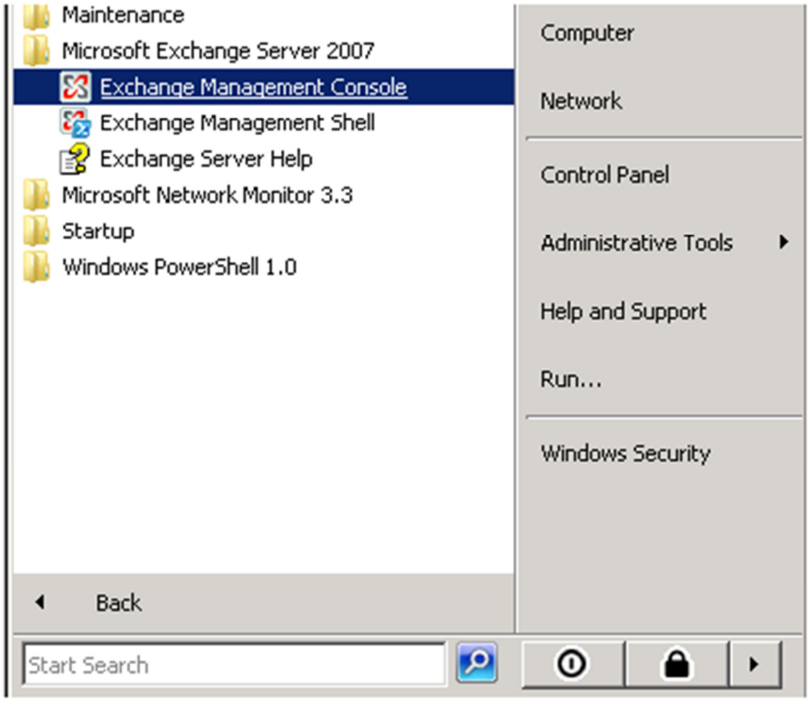
Exchange 2007:

To program the IP address restrictions on the receive connector in Exchange 2007:

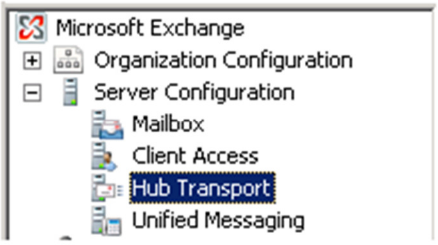
1. Obtain the list of ExchangeDefender IPs here:

65.99.255.0/24
64.182.140.0/24
206.125.40.0/24

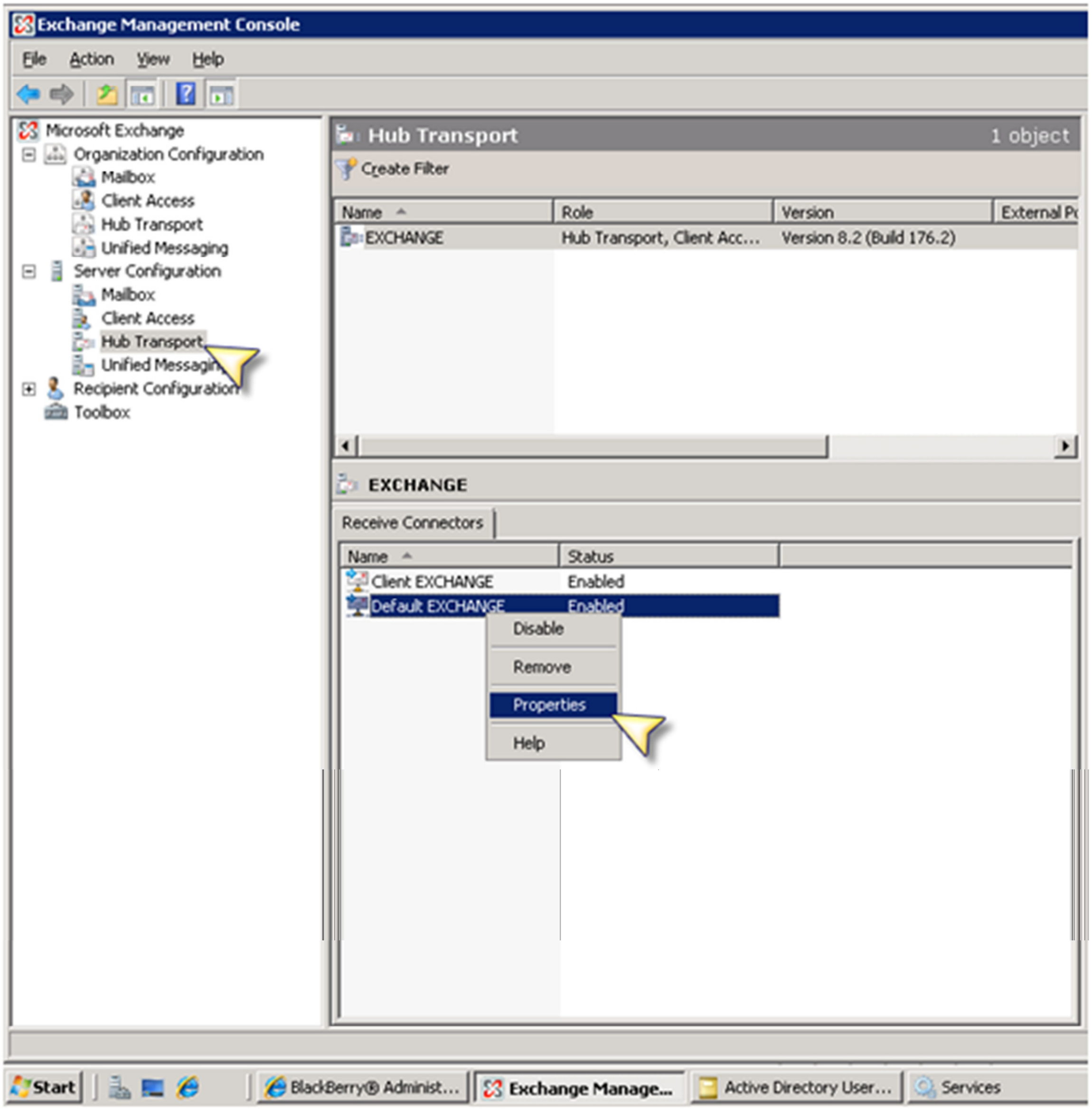
2. Open Exchange Management Console



3. Expand Server Configuration, click **Hub Transport**



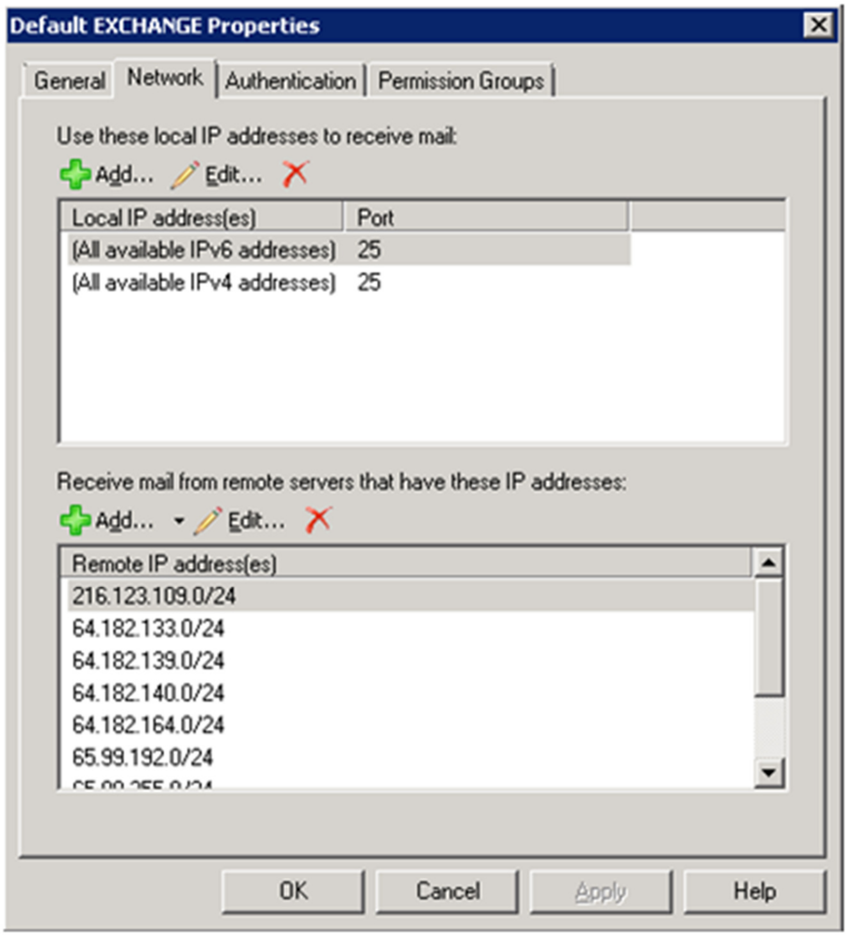
4. SBS Users: Right click on the *"SBS Internet Mail Connector"* and select Properties
NON-SBS Users: Right click on *"Default SERVERNAME"* and select *"Properties"*.



Name	Role	Version	External P
EXCHANGE	Hub Transport, Client Acc...	Version 8.2 (Build 176.2)	

Name	Status
Client EXCHANGE	Enabled
Default EXCHANGE	Enabled

5. Once the dialog box pops up select the *"Network"* tab:



Use these local IP addresses to receive mail:

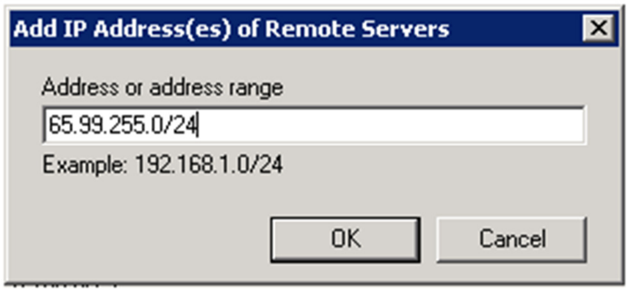
Local IP address(es)	Port
(All available IPv6 addresses)	25
(All available IPv4 addresses)	25

Receive mail from remote servers that have these IP addresses:

Remote IP address(es)
216.123.109.0/24
64.182.133.0/24
64.182.139.0/24
64.182.140.0/24
64.182.164.0/24
65.99.192.0/24

6. Under "Receive mail from remote servers that have these addresses:" find the entry that says *0.0.0.0-255.255.255.0* and **delete** the record.

7. Under "Receive mail from remote servers that have these addresses:" click **Add**. Input the first ExchangeDefender IP range/netmask. Repeat this step for each ExchangeDefender IP network in the deployment guide.



Address or address range: 65.99.255.0/24

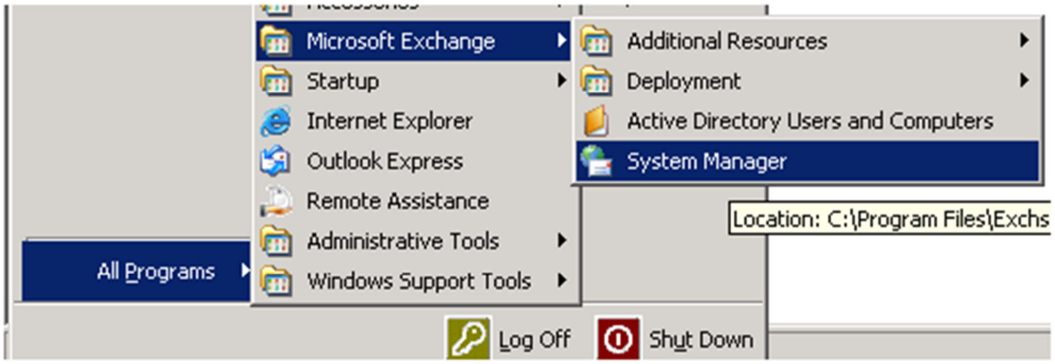
Example: 192.168.1.0/24

Exchange 2003:

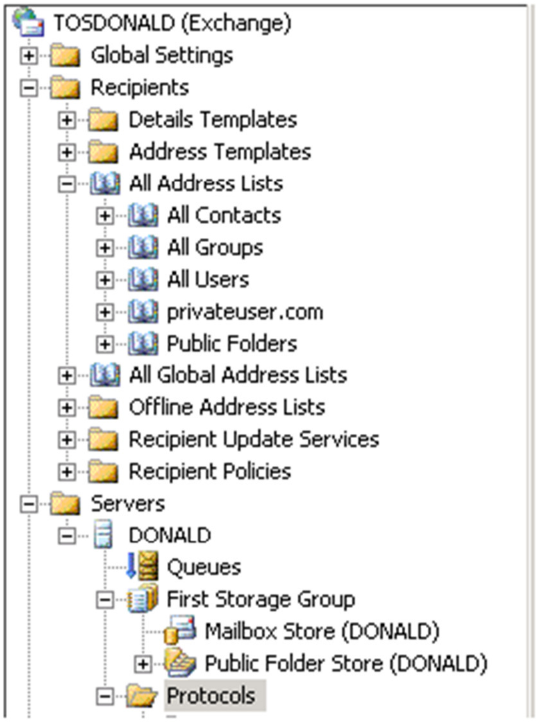
1. Obtain the list of ExchangeDefender IPs from here:

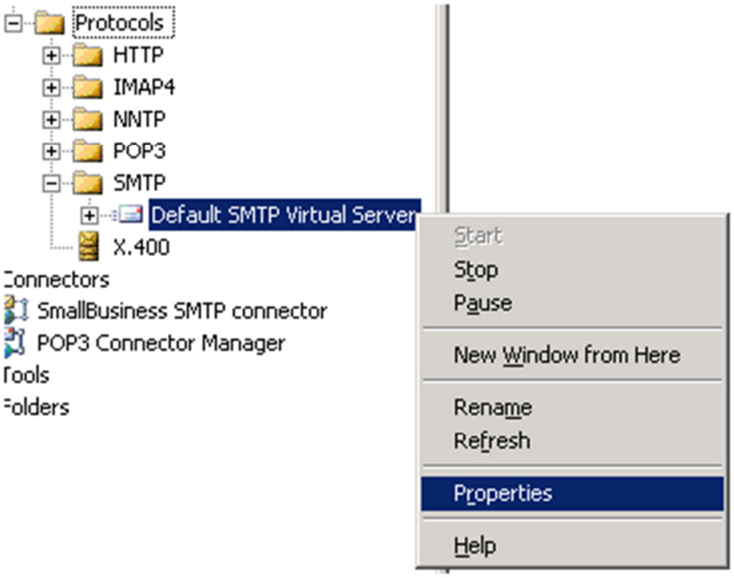
   65.99.255.0/24
   64.182.140.0/24
   206.125.40.0/24

2. Login to your Exchange 2003 server and open *System Manager*

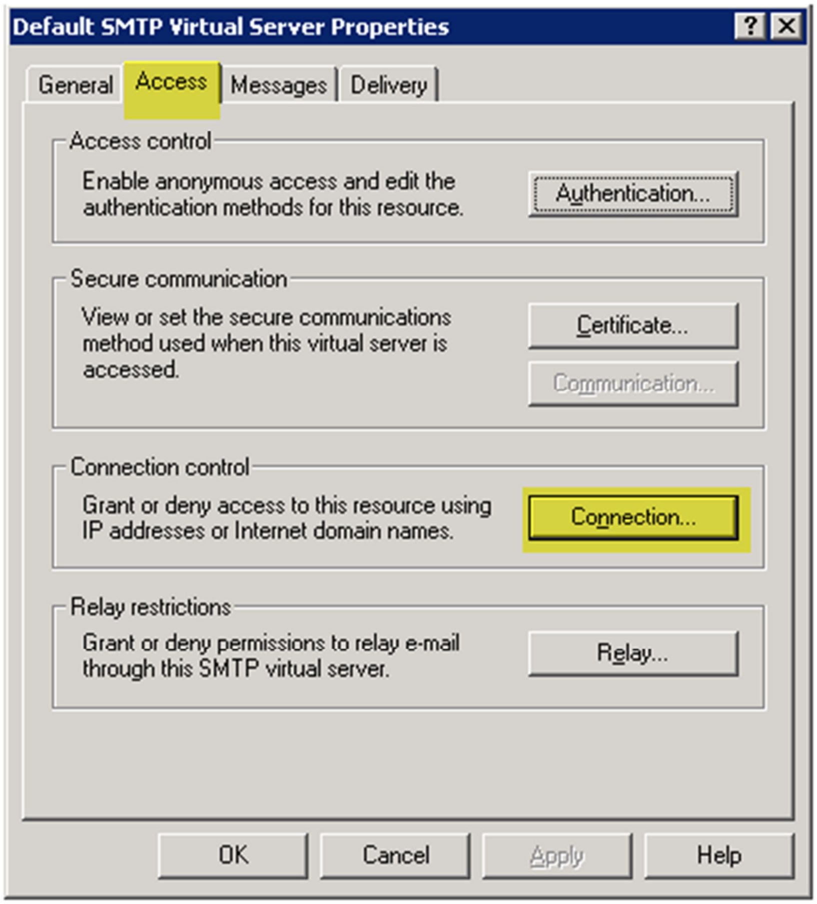


3. Expand Servers, ServerName, Protocols, SMTP - right click *"Default SMTP Virtual Server"* (Or the active receive connector name) and select properties





4. Navigate to the *Access tab* and then select the *Connection button*.



Enable anonymous access and edit the authentication methods for this resource.

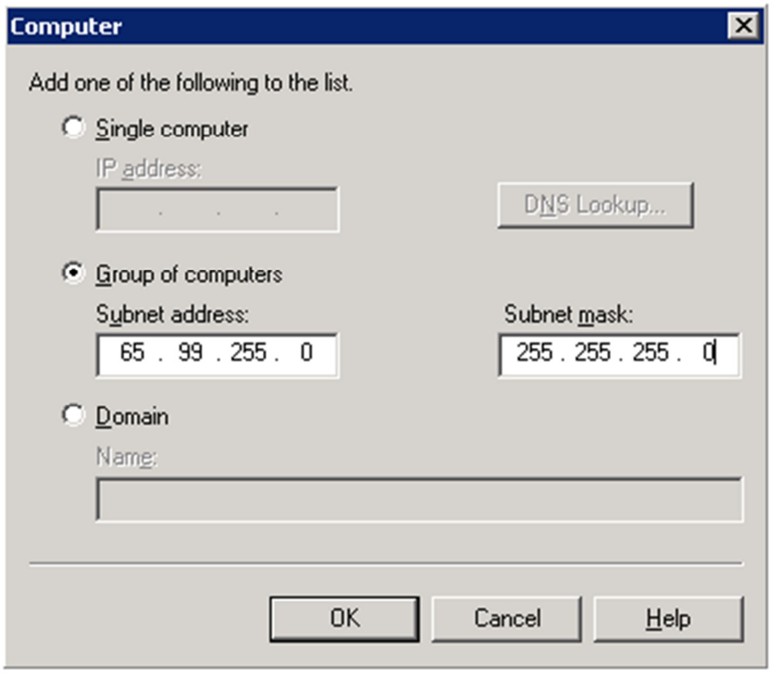
View or set the secure communications method used when this virtual server is accessed.

Grant or deny access to this resource using IP addresses or Internet domain names.

Grant or deny permissions to relay e-mail through this SMTP virtual server.

5. Remove any entries from previous providers or entries that have the IP range *0.0.0.0 - 255.255.255.0*

6. Click **Add** to enter a new IP restriction. Select the *Group of computers* option, insert the first IP range for ExchangeDefender and set the subnet mask to *255.255.255.0* - click **OK**. Repeat this step for each ExchangeDefender network.



Computer

Add one of the following to the list.

○ Single computer

IP address:

● Group of computers

Subnet address: 65 . 99 . 255 . 0

Subnet mask: 255 . 255 . 255 . 0

○ Domain

Name:

7. Restart the *Simple Mail Transfer Protocol (SMTP)* service to apply the changes.

Warning: Do not enforce IP restrictions until at least 72 hours after the MX record change. Enforcing IP restrictions while your old DNS zone is still cached on the Internet will result in a permanent mail loss and mail delays.

Should the IP restrictions be applied on the firewall or on the mail server? We are frequently asked this question and the answer depends on whether you have external users or third parties attempting to relay mail through your mail server. If you have external connections to your SMTP server (from third party vendors or mobile users) then it is easier to enforce restrictions on the mail server and enforce password protected SMTP access there. However, if you do not have external connections the restrictions should be enforced on the firewall in order to free up resources on the mail server.

Install Client Desktop Software

RoyAl Technology Management recommends deployment of Client Software Suite solutions over email Daily and Intraday digest reports for several reasons:

- Over 99% of all email SPAM reports are ignored or filtered to junk mail.
- Outlook and Desktop addins allow for realtime access to SPAM quarantines and settings.
- Client Desktop solutions work the way users do, in the applications they use.
- Client Desktop solutions are interruptive, they alert the users when necessary.

ExchangeDefender Client Software Suite was designed to give the user a more familiar experience, closely tied to the way they access their email and messaging. Outlook 2007 addin is perfect for Outlook power-users that never want to leave their Outlook experience. Similarly, Windows Desktop agent "annoyarizer" was designed for sales professionals, travel agents, financial industry employees and anyone that needs frequent alerts telling them that SPAM has been blocked from their inbox.

For more information about Client Software Suite please see the following page:

http://service.royaltechnologymanagement.com/downloads.php?action=displaycat&catid=10