Network configuration: IIS SMTP mail relay service and Microsoft Exchange Server

You can use the IIS SMTP mail relay service to prevent spammers from directly interacting with your Microsoft Exchange Server!

Your Exchange Server is probably set up on your internal network to receive all mail for users in your domain for onward delivery. If you publish your Exchange Server's SMTP service, Internet users can send messages directly to your Exchange Server. Allowing the Internet to have direct contact with your Exchange Server is never a good idea. To stop this direct contact, set up an IIS SMTP relay, and instead of publishing the Exchange Server's SMTP service, publish the IIS SMTP Service. Now when mail destined for yourdomain.com hits the external interface of your firewall, it will be forwarded to the SMTP relay. The SMTP relay in turn forwards it to your Exchange Server. Now set your Exchange Server to send outgoing SMTP mail messages to the IIS SMTP relay server so it forwards them on to the Internet.

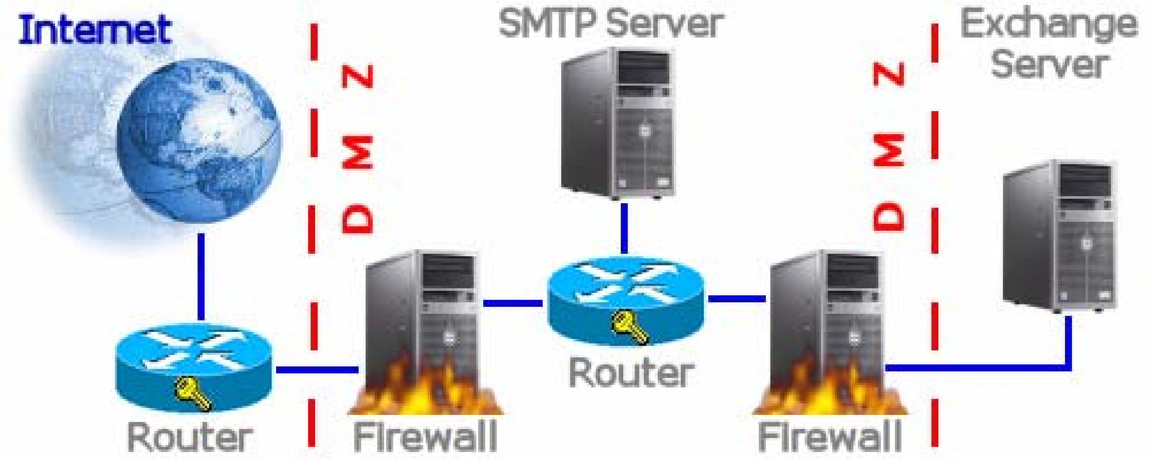

Figure 1: With this configuration, your Exchange Server's SMTP service never has to interact with an Internet SMTP server.

To secure this set up, for incoming mail, allow the IIS SMTP server to relay only to your own domains. For outgoing mail, allow the IIS SMTP server to relay to all domains. If you allow incoming mail to be relayed to all domains, spammers will take advantage of your open mail relay and you'll process thousands of spam e-mails within a few days. A default configuration allows all computers that can authenticate to relay through the server; however, authentication requires more overhead, so it's better to allow relay based on IP address. Since you only want to allow your Exchange Server to use the IIS SMTP Server as an open relay, add the IP address of your Exchange Server to Allow "Only the list below." You need to allow the IIS SMTP Service to act as an open relay for your Exchange Server because the Exchange Server needs to send SMTP mail to all Internet mail domains. The open relay for outbound mail is required. You also need to prevent relay for incoming messages. Do this by configuring the server to relay only messages destined to your own domain:
<ol>
<li> In the Internet Services Manager console, expand the Default SMTP Virtual Server node.
<li> Right-click on the Domains node, point to New and click Domain.
<li> Select the Remote option and click Next.
<li> Type in your mail domain name and click Finish.

<li> Double-click on your new Remote Domain name.
<li> Check the option to Allow incoming mail to be relayed to this domain so that inbound mail destined for other domains is dropped by the SMTP relay.
<li> In the Route domain frame, select Forward all mail to smart host.
<li> Enter the IP address of your Exchange Server in the text box under this selection in brackets, like [192.168.1.254].
</ol>

Another advantage of this set up is that you can take down the Exchange Server for maintenance without losing any incoming mail. You can also improve fault tolerance by setting up multiple IIS SMTP Servers. Another possibility would be to add an additional mail relay server to filter e-mail for spam or viruses before relaying it on to the Exchange Server.