mailguard

MAILGUARD HELP DESK: MailGuard and Microsoft Exchange 2007

MailGuard and Microsoft Exchange 2007

Contents

Introduction

Viruses are becoming more prevalent and sophisticated every day. Microsoft Exchange, when used in conjunction with MailGuard, can offer full protection from viruses even before they've been officially recognised and anti-virus software is capable of detecting them.

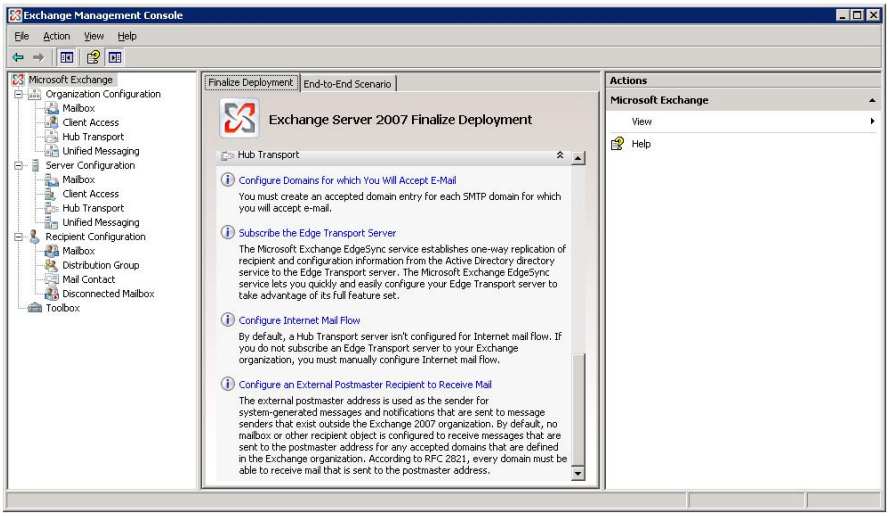
The section **Protecting OUTBOUND email** outlines the procedure for setting up your Microsoft Exchange server to direct all outbound email (that is, email originating from within your organisation) to MailGuard for scanning. Even if you are running anti-virus software locally, and despite the fact all your incoming emails are virus-free, there are many different ways a virus can infect a computer. Eliminate the possibility of virus emails originating from your company by sending all your outbound emails to MailGuard for scanning.

Virus authors commonly send infected emails directly to mail servers, bypassing the normal delivery mechanism (and hence our filter servers!). The only way to ensure that all of your emails have been delivered through the proper channels and verified by us as virus-free is to instruct your mail server to only accept email deliveries from MailGuard servers. Instructions for doing this are outlined in the section **Preventing unauthorised INBOUND email**.

The steps below are performed in the Microsoft Exchange Management Console application.

1. Start the Microsoft Exchange Management Console: **Start**, **All Programs**, **Microsoft Exchange Server 2007**, **Exchange Management Console** (see Figure 1).

Figure 1



Protecting OUTBOUND email

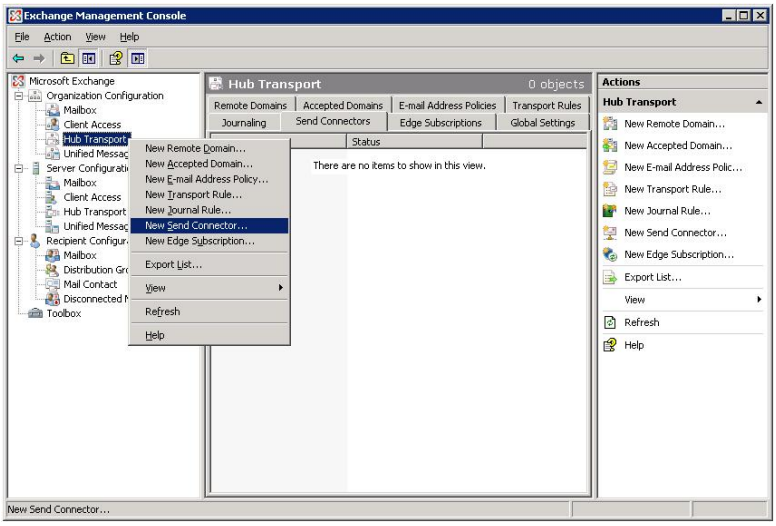
Note: the following steps outline the process of ensuring that all e-mail sent from your organisation via this Exchange server is delivered via MailGuard. Given the universal scope of this MailGuard Send Connector, you are advised to either disable or remove any existing Send Connectors to ensure that all mail is indeed routed via MailGuard.

If necessary, please consult your Administrator and amend the relevant steps should you require that certain mail be routed differently.

To configure Exchange to send all outbound messages (i.e. messages originating from within your organisation) to MailGuard for filtering, please perform the following steps:

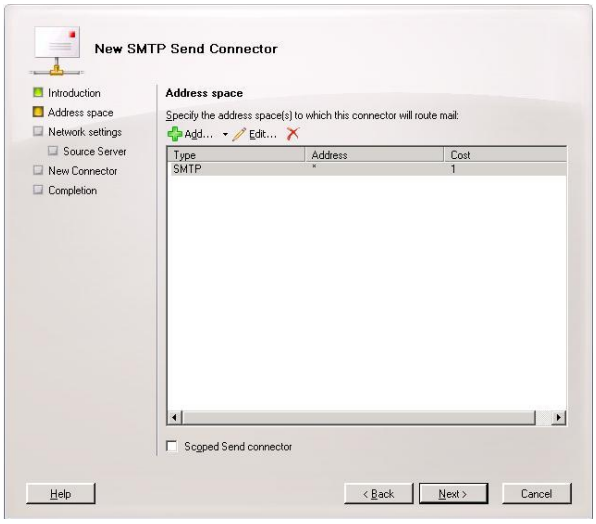
1. Open the Microsoft Exchange Management Console as detailed in the **introduction** of this document.
2. Create new SMTP Send Connector: Under Organisation Configuration, **right click** Hub Transport and then **left click** the resulting New Send Connector... option (see Figure 2).

Figure 2



3. Enter the desired Name for the new SMTP Send Connector e.g. MailGuard.
4. Ensure that the selected use for this Send Connector is set to Custom. Click **Next**.
5. **Add** a new SMTP Address Space. To ensure that this Connector will route mail to all domains enter the wildcard character * in the Address field. The **Include all subdomains** checkbox will default to checked given this Address.
   Leave the Cost field at the default value of 1. Click **OK.**
6. Under most typical configurations, the Scoped Send connector checkbox will remain unchecked. Consult your Administrator if you are unsure whether this Connector should be made available to all Hub Transport servers in the Exchange Organisation.
7. Click **Next** (see Figure 3).

Figure 3



8. Under Network Settings select the Route mail through the following smart hosts radio button. Click **Add**.
9. Under the Add smart host pop-up, select the Fully qualified domain name (FQDN) radio button.
10. Enter the name of your outgoing filter server. The name of your outgoing filter server takes the format:

    filter.xxxxxx-x.mailguard.com.au

    (where **xxxxxx-x** is the unique MailGuard code allocated to your domain).

    The name of your outbound filter server was included in the welcome message you received upon joining MailGuard.

    If you're not sure of the name of your outbound filter server, please **contact MailGuard Support** MailGuard Support or click on the **View** button next to your domain name in the **Domains** tag of the **MailGuard Management Console**.

11. Leave **Use the External DNS Lookup** settings on the transport server checkbox unchecked. Click **Next**.

12. Select the **Basic Authentication** radio button under the **host authentication** settings section.

13. Under most circumstances, ensure that the **Basic Authentication** over **TLS** checkbox is checked. Please consult your Administrator if you are unsure.

14. Enter the smart host **User name** and **Password**

    NOTE: This is not the same username and password you use to log into the MailGuard Management Console.

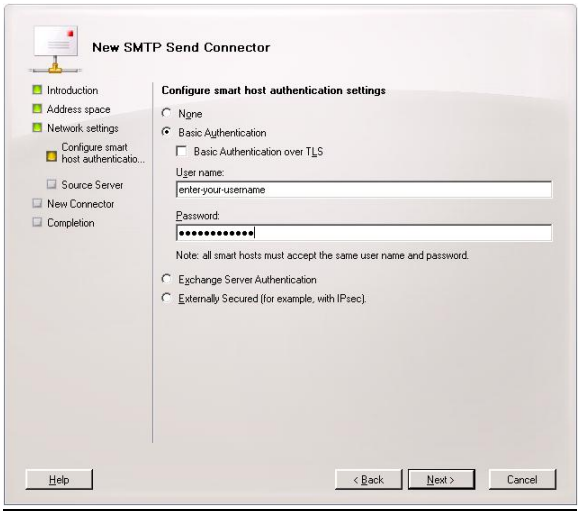
    Your SASL (also called SMTP authentication) username and password was included in the welcome letter you received upon joining MailGuard. If you don't have these details, please **contact MailGuard Support** or click on the **View** button next to your domain name in the **Domains** tag of the **MailGuard Management Console**.

15. Click **Next** (see Figure 4).

    MailGuard offers an alternative method of SMTP authentication. At your request, MailGuard can simply add your static IP to our trusted networks list. Under this configuration you should select an authentication method of None in step 12 above.

    Please note that we offer this alternative authentication method only to clients who have a static IP address. Please **contact MailGuard** should you qualify and have a preference for authenticating in this manner.

Figure 4

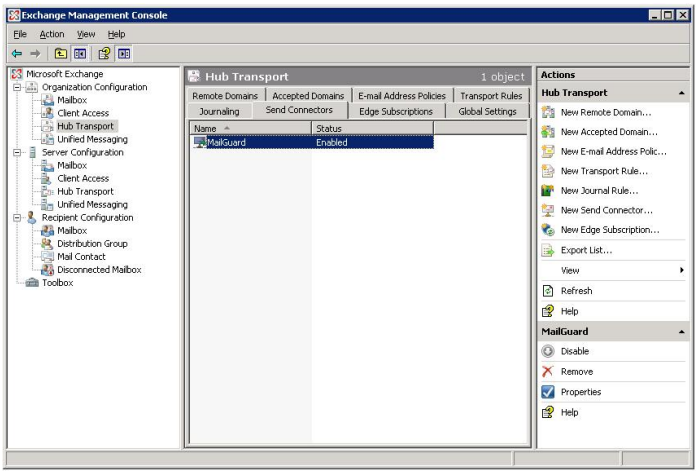


16. Should you only have a single **Exchange** server, simply click **Next** under the **Source Server** configuration page. Please consult your Administrator should you have a more complex configuration.

17. Review your **Configuration Summary** and correct any mistakes by cycling back through your configuration using the **Back** button. If each item is correct, click **New**.

18. Completion. Click **Finish** (see Figure 5).

Figure 5



MailGuard and Sender Policy Framework (SPF)

In computing, **Sender Policy Framework (SPF)** allows software to identify messages that are or are not authorised to use the domain name in the SMTP HELO and MAIL FROM (Return-Path) commands, based on information published in a sender policy of the domain owner. Forged return paths are common in e-mail spam and result in backscatter. (Source: wikipedia).

Should you currently utilise SPF, it is imperative that you amend each record associated with domains relaying mail via MailGuard.

To ensure that your SPF continues to function correctly, please add the following “include” string to your existing SPF: **include:customer.mailguard.com.au**

Preventing unauthorised INBOUND email

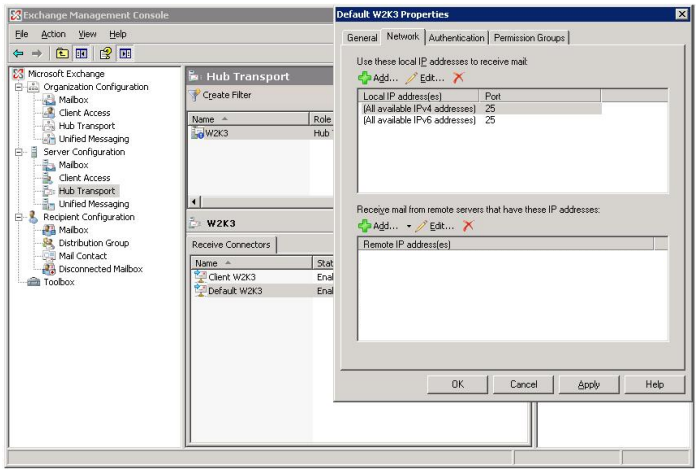
To prevent malicious users from delivering messages directly to your **Exchange Server** (thus bypassing MailGuard's servers), perform the following steps:

1. Open the **Microsoft Exchange Management Console** as detailed in the **introduction** of this document.
2. Left click the **Hub Transport** sub-item located under **Server Configuration**.
3. In the centre panel, double-click the **Default <Server Name> Receive Connector**.
4. Select the **Network** tab.
5. Under the **Remote IP address(es)** table, add each of the following IP Addresses exactly as below:

50.23.246.238/32
50.23.252.166/32
108.168.255.216/32
108.168.255.217/32
203.21.125.32/32
203.21.125.33/32

6. Ensure that all other unauthorised Remote IP address(es) are removed.
7. Completion. Click **OK**. (see Figure 6).

Figure 6



Contact MailGuard

For any queries, comments or suggestions regarding this guide, please feel free to contact the MailGuard Service Desk via **support@mailguard.com.au** or by calling 1300 30 65 10.