Step 6 - Routing Inbound Mail

https://campus.barracuda.com/doc/3866702/

The next step in setting up your Barracuda Email Security Gateway is to route incoming email to the system so it can scan incoming messages for spam and viruses. **Note that inbound mail will be blocked if the domain receiving the mail has not been configured on the Email Security Gateway.** To configure domains, see Creating and Managing Domains.

Important: In addition to this article, if you are using:

- Google Workspace Business and Education editions with the Barracuda Email Security Gateway as your inbound mail gateway, please see How to Configure Google Workspace for Inbound and Outbound Mail in addition to reading this article.
- Amazon Web Services, see Routing Mail Through Amazon Web Services

You can use either of the following methods to route messages to your Barracuda Email Security Gateway:

- Use **port forwarding** to redirect incoming SMTP traffic (port 25) to the Barracuda Email Security Gateway if it is installed behind a corporate firewall running NAT (Network Address Translation). For more information about port forwarding, refer to your firewall documentation or network administrator.
- **MX records** are used when your Barracuda Email Security Gateway is located in a DMZ with a routeable public IP address. If your Barracuda Email Security Gateway is in the DMZ (not protected by your corporate firewall), do the following to route incoming messages to the system:

1. Create a DNS entry for your Barracuda Email Security Gateway. The following example shows a DNS entry for a Barracuda Email Security Gateway with a name of `barracuda` and an IP address of `66.233.233.88`:
   ```
   barracuda.yourdomain.com   IN   A   66.233.233.88
   ```
2. Change your DNS MX Records. The following example shows the associated MX record with a priority number of 10:
   ```
   IN MX 10 barracuda.yourdomain.com
   ```
   You can configure specific SMTP settings from the **ADVANCED > Email Protocol** page. After you route incoming email to the Barracuda Email Security Gateway, it will begin filtering all email it receives and routing good email to your mail server.

Testing Spam and Virus Scanning With a Local User Set

With the Barracuda Email Security Gateway 400 and higher, you have the option to use the **Explicit**

Users to Scan For feature to test a subset of locally defined users before fully deploying the Barracuda Email Security Gateway. See the **ADVANCED > Explicit Users** page.

To tune your spam settings, continue with How to Tune and Monitor the Default Spam and Virus Settings.

If you will be routing outbound mail through the Barracuda Email Security Gateway, continue with Routing Outbound Mail.