Google Workspace Journaling

https://campus.barracuda.com/doc/50266205/

> This article refers to Barracuda Message Archiver version 5.0 and higher, and Google Workspace.

Use the steps in this article to configure Google Workspace to send journal mail to the Barracuda Message Archiver.

Step 1. Ensure Public Access to Port 25 on the Barracuda Message Archiver

To Journal mail directly from Google Workspace to your Barracuda Message Archiver, you must have a public IP address and port 25 open and NATed to the Barracuda Message Archiver. Additionally, you can optionally have a public DNS record. You can test this by attempting to telnet to the Barracuda Message Archiver on port 25. You can expect one of three outcomes:

1. If the Barracuda Message Archiver is *not accessible*, either due to port 25 being blocked or incorrectly configured on the firewall, the attempt to telnet simply hangs at **Trying [IP address]**. In this case you need to troubleshoot your network settings:

    ```
    $telnet 104.209.184.162 25
    Trying 104.209.184.162...
    ```

2. If the Barracuda Message Archiver is *accessible* and you have set **Allow Only Trusted Hosts** on the **Mail Sources > SMTP** page to **No**, telnet establishes a connection to the Barracuda Message Archiver:

    ```
    $telnet 104.209.184.162 25
    Trying 104.209.184.162...
    Connected to 104.209.184.162.
    Escape character is '^]'.
    220 barracudaV650.getcuda.com ESMTP Barracuda; Mon, 14 Sep 2015 12:08:12 -0700 (PDT)
    ```

3. If the Barracuda Message Archiver is *accessible*, you have set **Allow Only Trusted Hosts** on the **Mail Sources > SMTP** page to **Yes**, and you are attempting to telnet from an IP address not listed in the **TRUSTED SMTP SERVERS** section, telnet establishes a connection and the connection is immediately closed:

    ```
    $telnet 104.209.184.162 25
    Trying 104.209.184.162...
    Connected to 104.209.184.162.
    Escape character is '^]'.
    550 Sender Not Recognized
    Connection closed by foreign host.
    ```

Step 2. Add Google IP Address Ranges to the Trusted SMTP Servers List

Google Workspace mail servers use a large range of IP addresses which may change. To determine the current Google IP address range, see the [Google IP address ranges for outbound SMTP](#) in the Google Workspace Administrator Help .

1. Use the steps outlined in the [Google IP address ranges for outbound SMTP](#) article.
2. Log in to the Barracuda Message Archiver as the administrator, and go to the **Mail Sources > SMTP** page.
3. Click **Bulk Edit**.
4. Copy and paste the IP addresses based on your region, and click **Save** .

Step 3. Configure SMTP Forwarding Settings

Because this configuration requires the Barracuda Message Archiver to be public-facing, Barracuda Networks strongly recommends that you configure the Barracuda Message Archiver to only accept mail from the list of Trusted SMTP Servers. If you are also receiving mail from sources other than Google Workspace, make sure you add those IP addresses to the list of Trusted SMTP Servers before setting the Barracuda Message Archiver to **Allow Only Trusted Hosts**.

To configure SMTP forwarding settings,

1. Log into the Barracuda Message Archiver as the administrator, and go to the **Mail Sources > SMTP** page.
2. In the **SMTP Forwarding Settings** section, set **Allow Only Trusted Hosts** to **Yes**.
3. Click **Save**.

Step 4. Configure Local Domains

1. Log into the Barracuda Message Archiver as the administrator, and go to the **Basic > IP Configuration** page.
2. In the **Local Domains** section, add all of your mail-enabled domains.
3. Click **Add** after each domain entry, and click **Save**.

Step 5. Configure SMTP Over TLS/SSL *(Optional)*

1. Log into the Barracuda Message Archiver as the administrator, and go to the **Advanced > SMTP Configuration** page.
2. In the **SMTP Over TLS/SSL** section, set **Enable SMTP over TLS/SSL** to **Yes**.
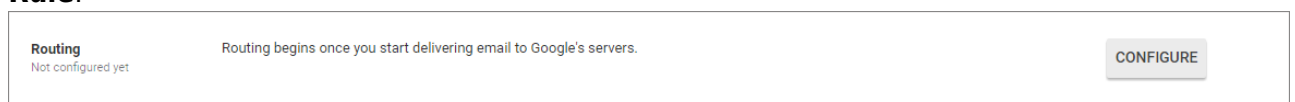3. Click **Save**.

Step 6. Add Route

1. Sign into the Google Workspace domain console, and go to **Apps > Google Workspace > Gmail > Hosts** .
2. Click **Add Route**.
3. In the **Add mail route** page, enter your Barracuda Message Archiver settings:
   1. Type `Barracuda Message Archiver` in the **Name** field.
   2. In the **Specify email server** section, enter your Barracuda Message Archiver public IP address or public DNS record.

      > You can optionally select **Require secure transport (TLS)**. When selected, you must set **Enable SMTP over TLS/SSL** to **Yes** on the **Advanced > SMTP Configuration** page in the Barracuda Message Archiver web interface (see *STEP 5* above).
      > If you are using a self-signed certificate, clear **Require CA signed certificate**.
4. Click **Save**.
5. Go to **Apps > Google Workspace > Gmail > Routing**. Click **Configure** or **Add Another Rule**.

Routing Not configured yet	Routing begins once you start delivering email to Google's servers.	CONFIGURE

6. Enter a unique name to identify the setting, and select all of the check boxes under **Messages to affect**:
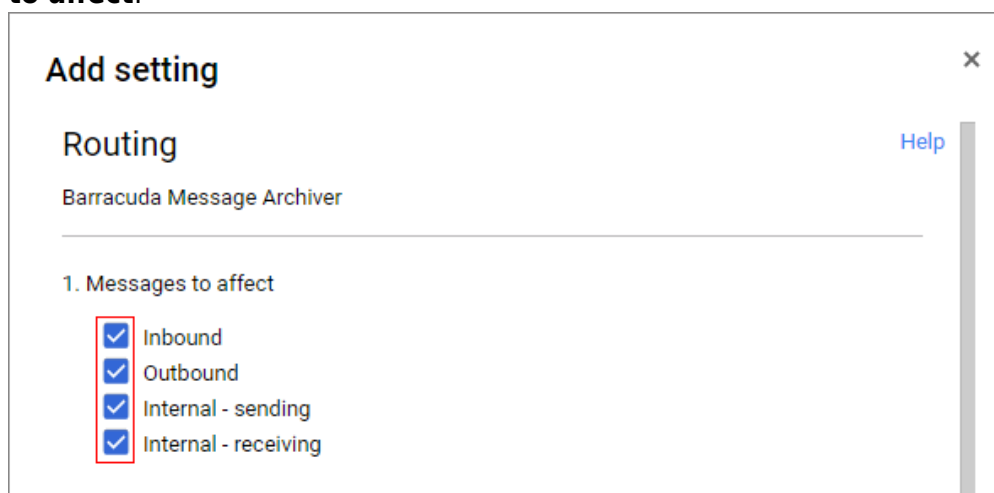
7. Scroll to **Also deliver to**, click **Add more recipients**, and click **Add**.

8. Under **Recipients**, select **Advanced** from the drop-down menu.
9. Select **Change route** and **Barracuda Message Archiver**.
10. Clear **Do not deliver spam to this recipient** and select **Suppress bounces from this recipient**.
11. Click **Save**, and click **Add Setting**.
12. Click **Save**:

| Routing
Locally applied | Barracuda Message Archiver

Messages: All
Filters: None
Consequences: Modify message, Additional delivery: 1 | EDIT | DISABLE | DELETE | ADD ANOTHER | COPY TO ORGANIZATION |

Figures

1. telnet_port_25_blocked.png
2. telnet_port_25_open_all.png
3. telnet_port_25_openO365.png
4. routing.png
5. messages_to_affect.png
6. final.png