Step 2 - Deploy Compliance Edition for G Suite

https://campus.barracuda.com/doc/74550011/

Use this article to deploy Barracuda Email Security Service and Advanced Threat Protection for G Suite in your environment.

To deploy Barracuda Essentials with G Suite, you must have a G Suite Basic, Business, or Enterprise account. The legacy free edition of G Suite is missing key features required for this deployment. For details on upgrading your G Suite subscription, refer to the Google Support article G Suite legacy free edition.

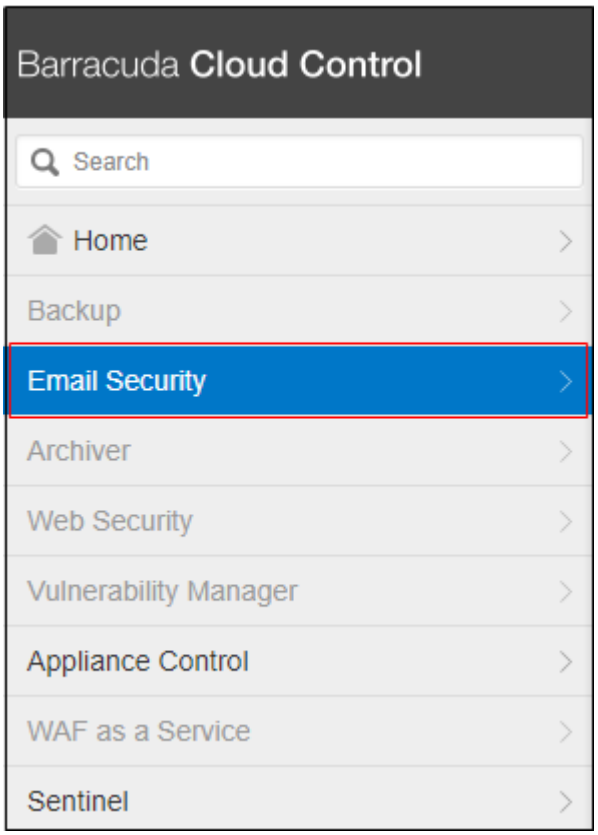
Google IP addresses and user interfaces can change; refer to the G Suite Administrator Help Center for updates and configuration details.

You can specify the Barracuda Email Security Service as an *inbound mail gateway* through which all incoming mail for your domain is filtered before reaching your Google account. The Barracuda Email Security Service filters out spam and viruses, then passes the mail on to the Google mail servers. Use the **Configure Inbound Mail Flow** instructions below to configure.

You can also specify the Barracuda Email Security Service as the *outbound mail gateway* through which all mail is sent from your domain via your Google account to the recipient. As the outbound gateway, the Barracuda Email Security Service processes the mail by filtering out spam and viruses before final delivery. By configuring Google as described in **Configure Outbound Mail Flow** below, you instruct the Google mail servers to pass all outgoing mail from your domain to the Barracuda Email Security Service (the gateway server).

Step 1. Launch the Barracuda Email Security Service Setup Wizard

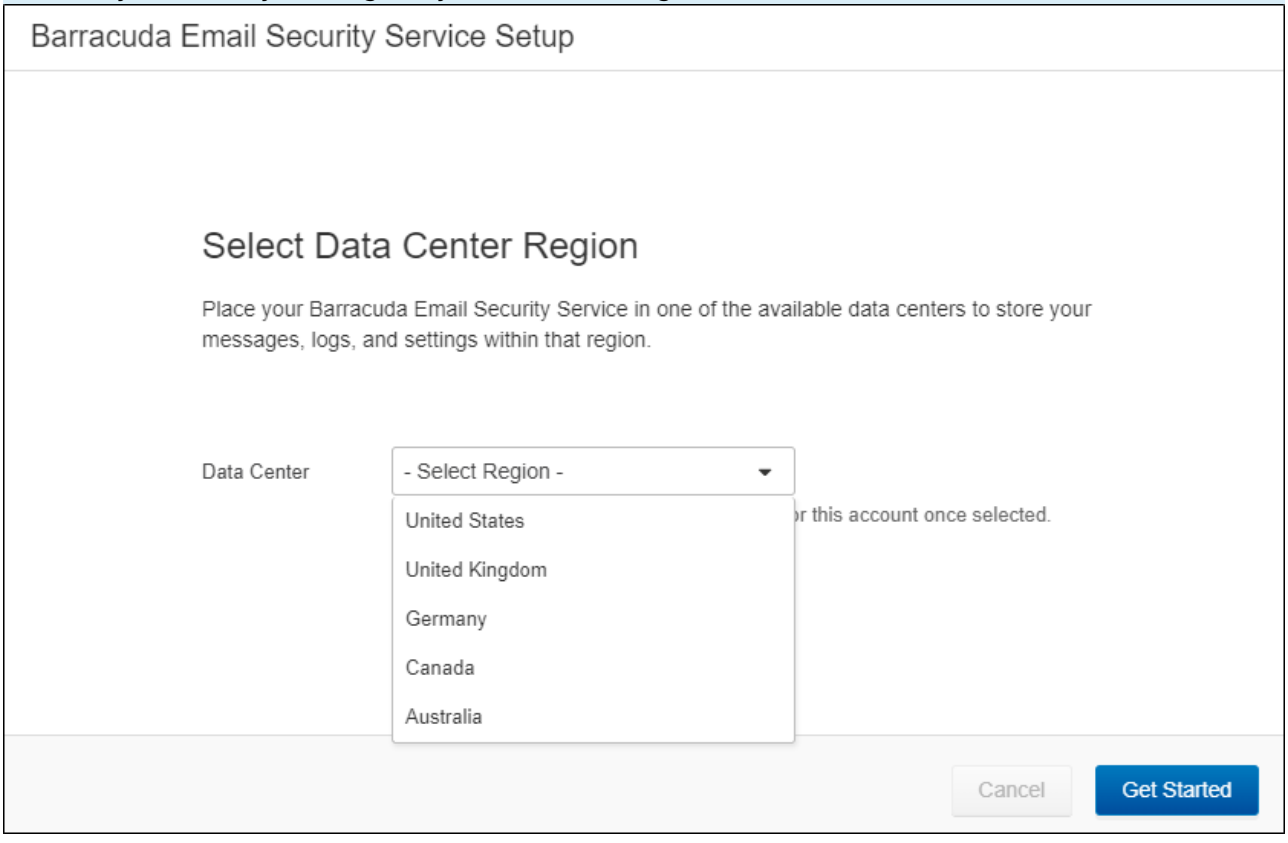
1. Log into your Barracuda Cloud Control account. On the left side, select **Email Security**.



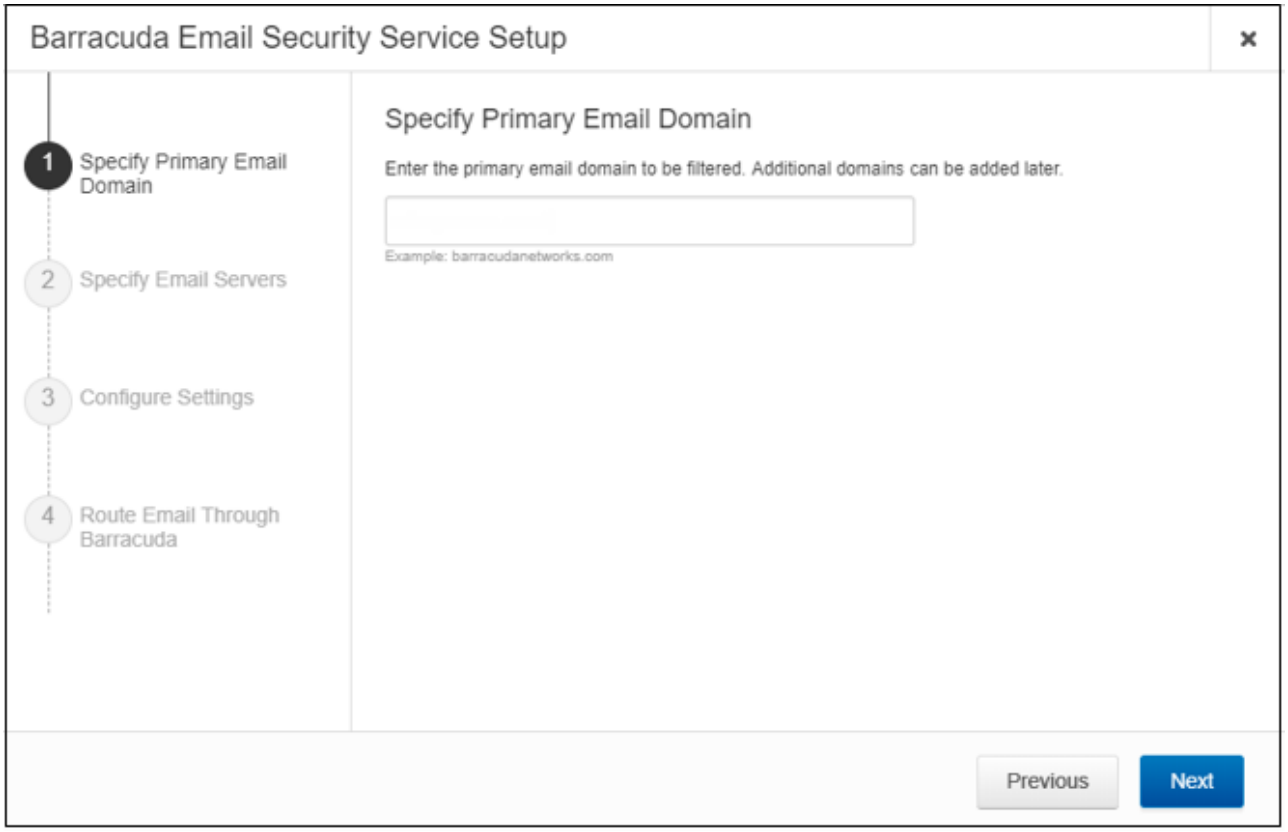
The Email Security wizard launches. Click **Next**.

2. Select the **Region** for your Data Center. Then click **Get Started**.

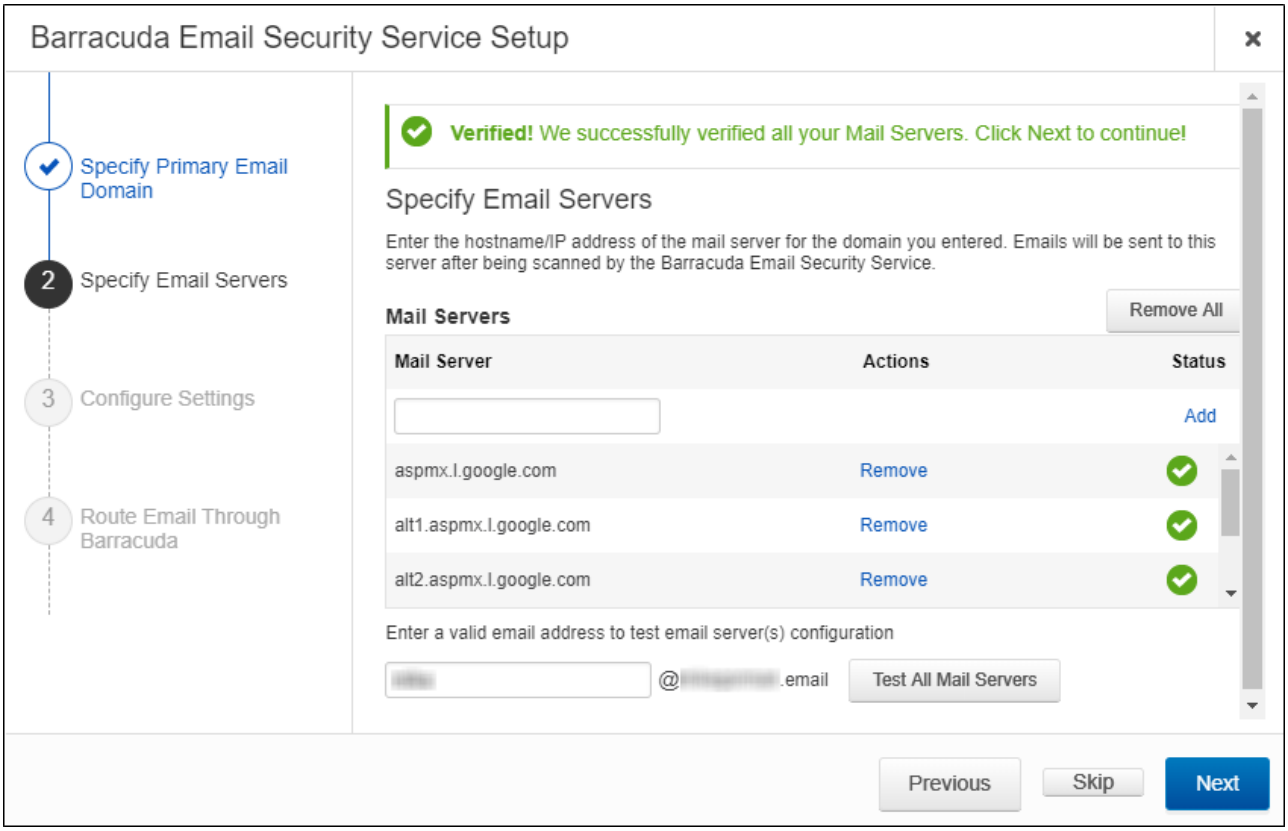
   After you select your Region, you cannot change it.



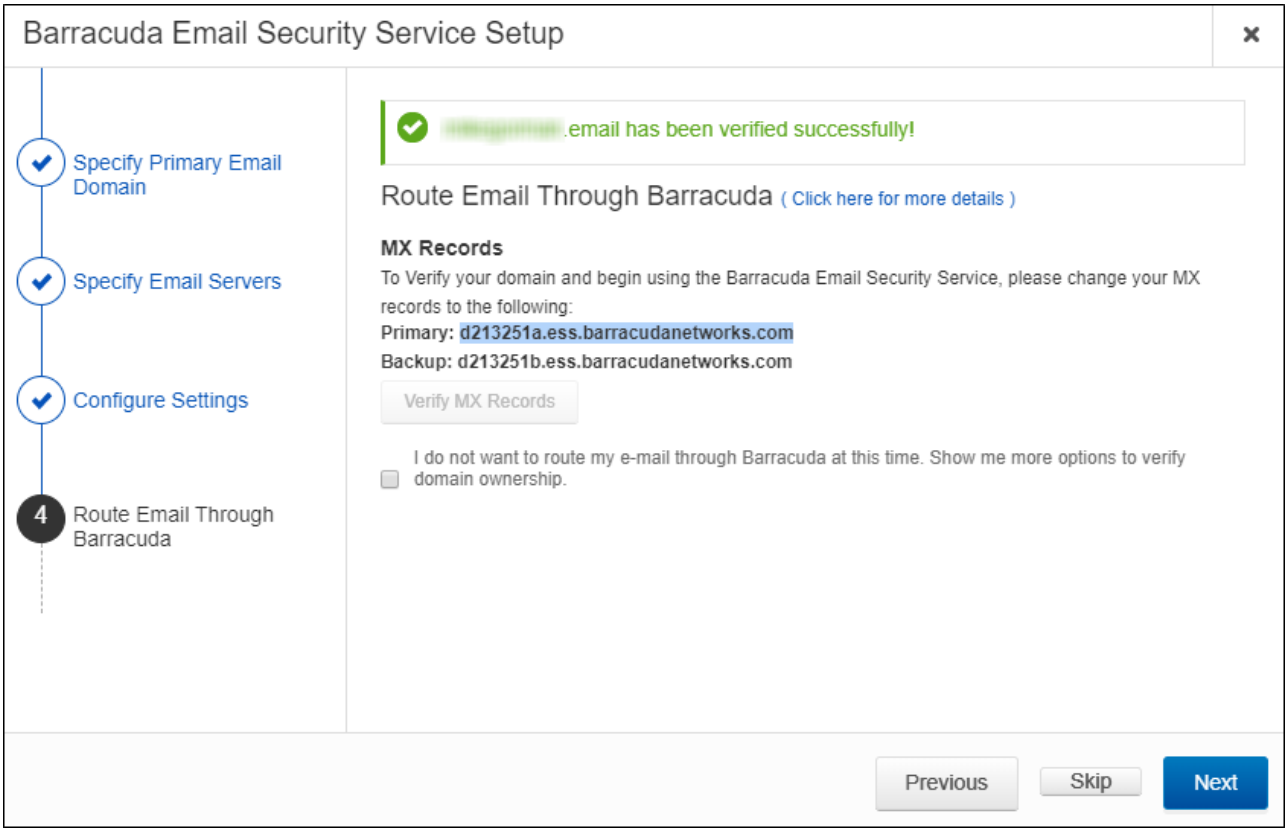
3. Enter the primary email domain you want to protect with Barracuda Email Security Service. Then click **Next**.



4. The system automatically retrieves your current MX records and auto-fills that information as your Destination Server. If this is not the correct Destination Server, click **Remove** and add the Destination Server with the correct data.
   If you want to add additional servers, enter data for those servers now.
   After you properly configure the Destination Server, enter a valid User Name to test the mail server connection.
   After you have determined that the settings are correct, click **Next**.



5. Select your settings, accepting the default values or making changes if needed, then click **Next**.
6. Barracuda Networks recommends verifying your domain via MX records with Priority 99. If you do not want to update MX records now, check the box and select a different method.
   In the first case, click **Verify MX Records**. Otherwise, click **Confirm Validation**.
   > Note that after verifying your domain, any mail sent to your domain from another Barracuda ESS customer will be processed normally by your ESS account and not delivered via MX records.
7. When the verification is successful, click **Next**.



If the verification is not successful, a message appears, letting you know that the domain could not be verified.
If you are having DNS issues that you want to address, click **Skip** to exit the wizard. Behind the wizard, click the **Domains** tab to retry the validation.

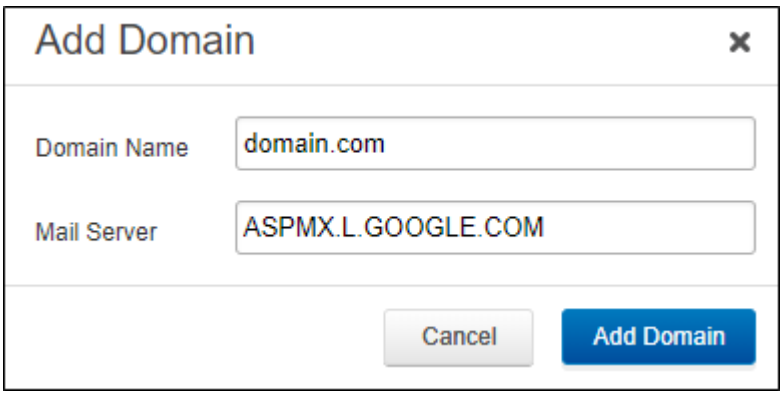
8. Click **Finish** to finalize the setup and close the wizard.

Step 2. Add Additional Email Domains *(Optional)*

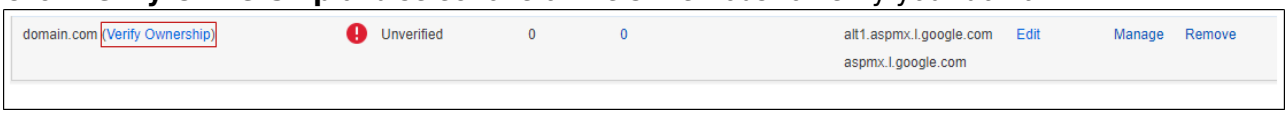
You configured your primary email domain in Step 3 of the wizard, above.

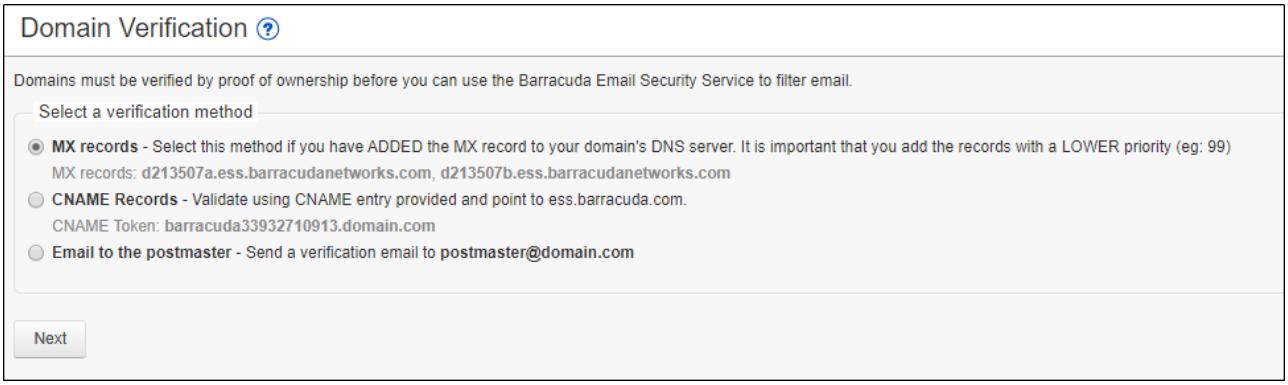
Use the steps in the following section if you want to protect additional domains with Barracuda Email Security Service. If you are only protecting one domain, continue below with *Step 3. Configure Inbound Mail Flow*.

1. Log into the Barracuda Cloud Control as administrator. In the left panel, click **Email Security**. Select the **Domains** tab, then click **Add Domain**.
2. Enter the domain name and the Primary MX record for Google: (see Table 1 below).



3. Click **Add Domain**; the **Domain Settings** page displays, listing the new domain.
4. Click **Add Mail Server** and add the remaining four mail servers from Table 1 below.
5. Click **Save Changes** and then click the **Domains** tab at the top.
6. Click **Verify Ownership** and select one of the 3 methods to verify your domain.





7. Repeat these steps, as needed, for additional domains before continuing with Step 3 below.
8. After the mail server is verified, the **Verified** icon displays in the **Status** column and a confirmation message displays at the top of the page.

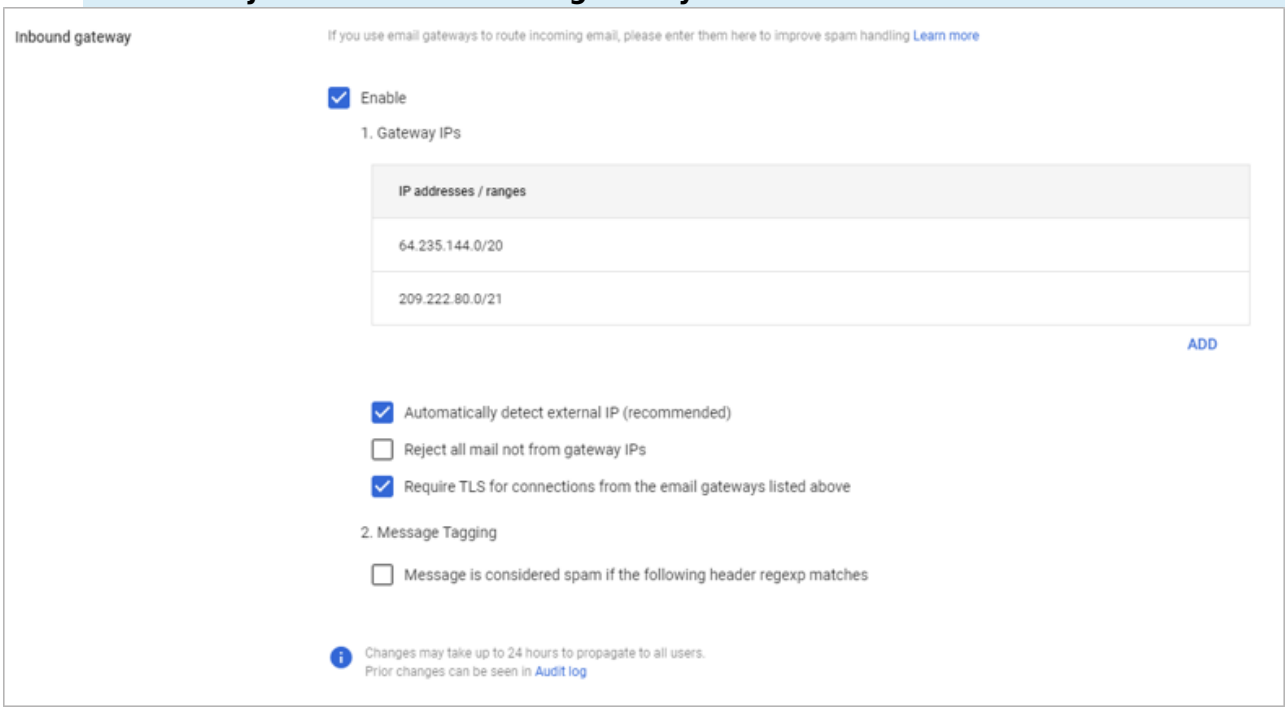
Table 1. G Suite Destination Mail Servers

Priority	G Suite Destination Mail Server
10	aspmx.l.google.com
20	alt1.aspmx.l.google.com
20	alt2.aspmx.l.google.com
30	alt3.aspmx.l.google.com
30	alt4.aspmx.l.google.com

Step 3. Configure Inbound Mail Flow

Before completing the steps in this section, verify your MX records display in the Barracuda Email Security Service MX records; otherwise mail delivery issues may be introduced.

1. Log into the G Suite admin console at https://admin.google.com.
2. From the **Home** page, go to **Apps > Google Workspace > Gmail**.
3. Select **Spam, Phishing and Malware** from the list.
4. Click **Inbound gateway**, and select the **Enable** check box.
   Note: If you have an inbound gateway configured, you need to add only the Barracuda IP ranges.
5. Click **Add** under **Gateway IPs**.
6. Enter the IP address/range for your Barracuda region.
   For example, if you are in the US region, type `64.235.144.0/20`, click **Save**. Click **Add** and then type `209.222.80.0/21`. Click **Save** again.
   For other regions, refer to the IP addresses listed in Barracuda Email Security Service IP Ranges.
7. Select the following options:
   1. **Automatically detect external IP (recommended)**
   2. **Require TLS for connections from the email gateways listed above**
      Note: if you are routing internal mail through Barracuda (default), you must also select **Reject all mail not from gateway IPs**.



8. Click **Save**.

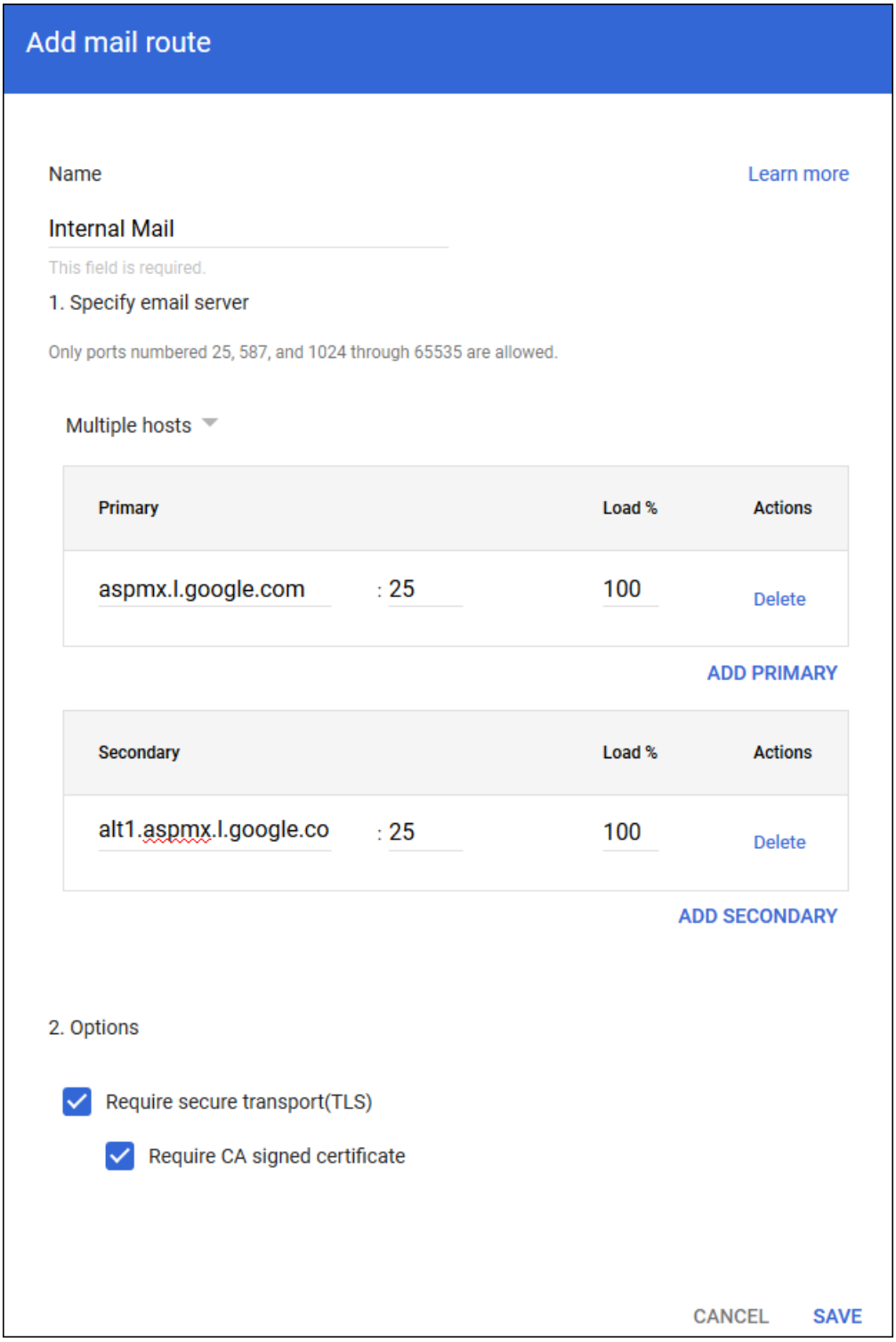
Step 4. Internal Mail

By default, your internal mail is sent out to your inbound MX record, which points to the Barracuda Email Security Service. This is by design for Google mail systems. To ensure that your internal mail stays internal, you must create a routing rule.

To configure a routing rule, follow the instructions below:

Step 1. Create Local Host

1. Log into the G Suite admin console at https://admin.google.com.
2. From the **Home** page, go to **Apps > Google Workspace > Gmail**.
3. Click **Hosts**.
4. Click **Add Route**. Enter a route name. For example, "Internal Mail".
5. Select **Multiple hosts**.
6. Enter the following **Primary host** details, and then click **Add Primary**.
    1. **Hostname** – aspmx.l.google.com
    2. **Port** – 25
    3. **Load**– 100%
7. Enter the following **Secondary host** details, and then click **Add Secondary**.
    1. **Hostname** – alt1.aspmx.l.google.com
    2. **Port** – 25
    3. **Load**– 100%
8. Under **Options**, select **Require secure transport(TLS)** and **Require CA signed certificate**.

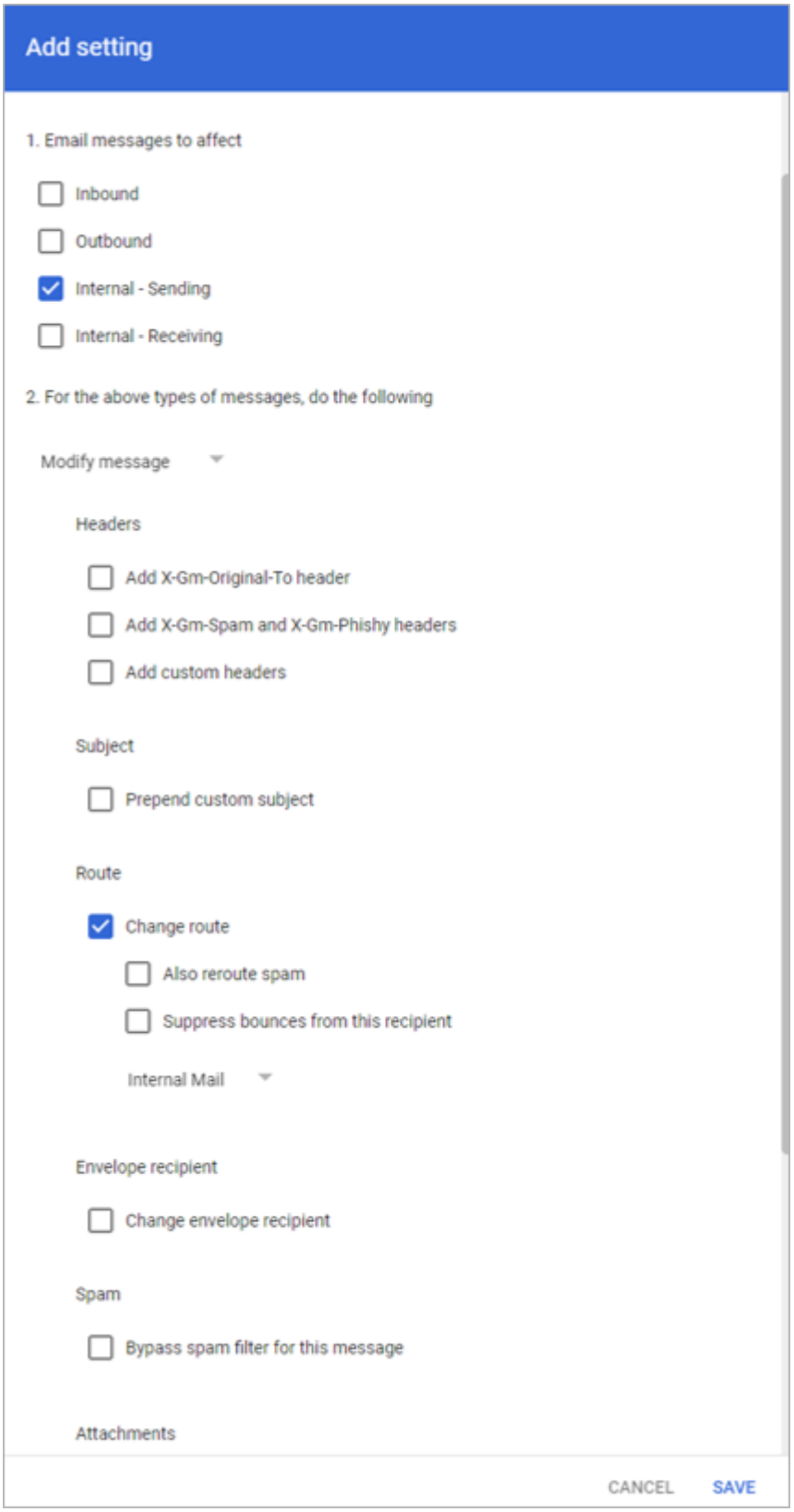


9. Click **Save**.

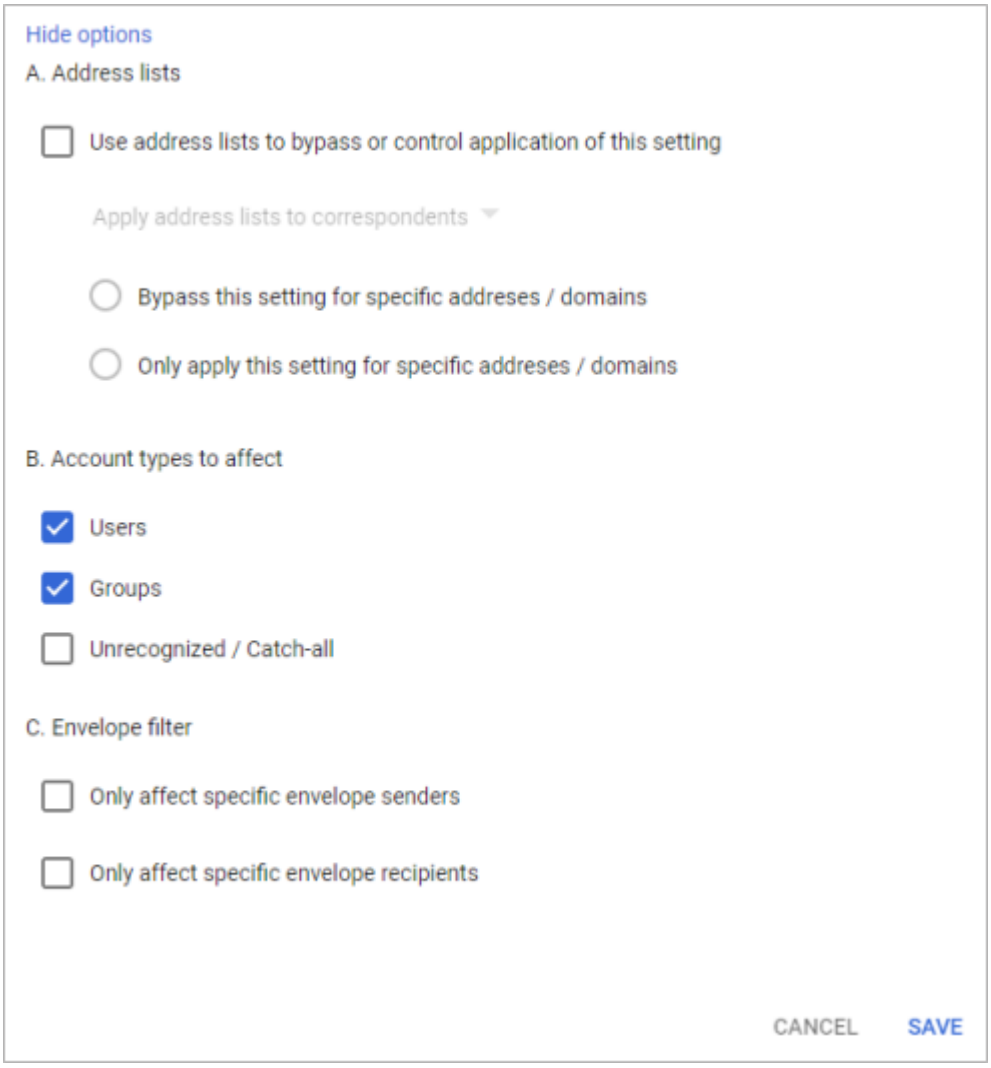
Step 2. Create Routing Rule

1. Navigate to **Apps > Google Workspace > Gmail**.
2. Click **Routing** at the bottom of the page.
3. Under the **Routing** section, click **Configure**.

4. Enter a name for the rule. For example, "Internal Mail".
5. Under **Email messages to affect**, select **Internal - Sending**.
6. Under **For the above types of messages, do the following**, click the Down arrow and then select **Modify message**.
    1. Select **Change route**.
    2. From the list of options, select the host you created above in *Step 1. Create a Local Host*.

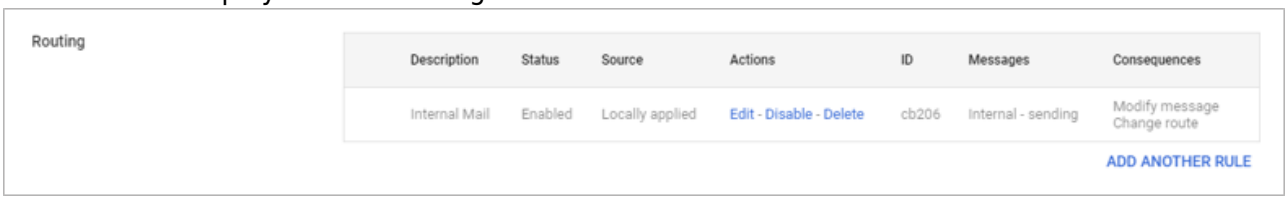


7. Toward the bottom, click **Show options**. Under **Account types to affect**, select **Users** and **Groups**.



8. Click **Save**.

   The new rule displays in the Routing section.



Step 5. Configure Sender Policy Framework for Outbound Mail

To ensure Barracuda Networks is the authorized sending mail service of outbound mail from your Barracuda Email Security Service, add the Sender Policy Framework (SPF) record INCLUDE line of the SPF record for your sending mail server for each domain sending outbound mail. See Sender Policy Framework for Outbound Mail for INCLUDE entries based on your Barracuda Email Security Service instance.

For example, your record will look similar to: `v=spf1 include:_spf.google.com include:spf.ess.barracudanetworks.com -all`

- If you have an SPF record set up for your domain, edit the existing record, and add the following to the INCLUDE line for each domain sending outbound mail based on your Barracuda Email Security Service instance. For example: `include:spf.ess.barracudanetworks.com -all`
- If you do not have an SPF record set up for your domain, use the following value to create a TXT record that creates a HARD Fail SPF for your domain based on your Barracuda Email Security Service instance. For example: `v=spf1 include:spf.ess.barracudanetworks.com -all`

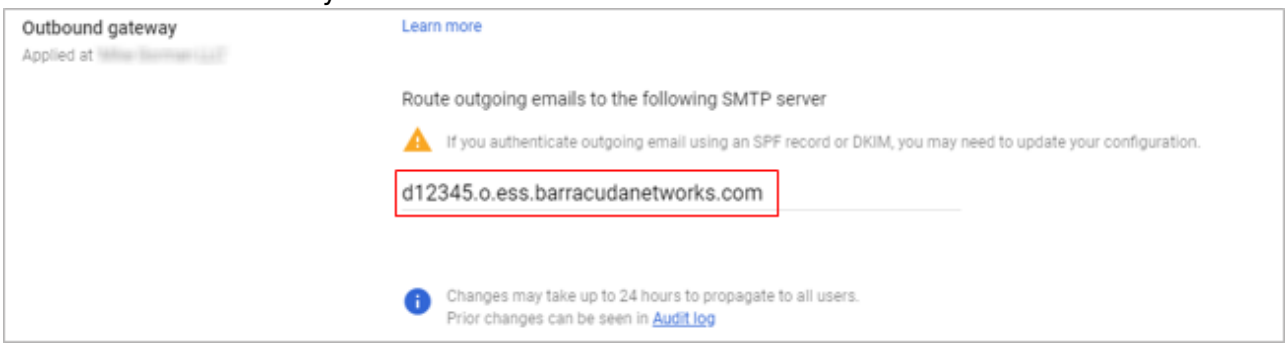
For more information, see Sender Authentication.

Step 6. Configure Outbound Mail Flow *(Optional)*

To ensure outbound mail delivery, contact Barracuda Networks Technical Support to have **Hosted Outbound Relay** enabled on your account. Failure to do so will result in undeliverable messages.

The steps in this section are taken from G Suite Admin Help.

1. Navigate to **Apps > Google Workspace > Gmail**.
2. Click **Routing** toward the bottom of the page.
3. Click **Outbound gateway**.
4. Enter the Outbound smart hostname provided to you in the settings for your domain within the Barracuda Email Security Service interface:



5. Click **Save** in the bottom right corner.

Continue with Step 3 - Deploy Compliance Edition for G Suite to deploy the Barracuda Cloud Archiving Service component.

Figures