Step 2 - Deploy Compliance Edition for G Suite

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 optionally whitelist the Barracuda Email Security Service IP ranges through G Suite Advanced settings. See Barracuda Email Security Service IP Ranges for a list of IP ranges based on your Barracuda Email Security Service instance.

Step 1. Launch the Barracuda Email Security Service Setup Wizard

Alternatively, you can manually set up the Barracuda Email Security Service using the web interface.

Click here to see more

Configure Domain

1. Log in to Barracuda Email Security Service, and go to the **Domains** page.
2. Under **Domain Name**, enter the primary email domain to be filtered.
3. Enter the primary G Suite destination mail server: ASPMX.L.GOOGLE.COM
4. Click **Add**.
5. Click **Add Mail Server** to continue adding the remaining G Suite destination servers and their respective priority:

Priority	G Suite Destination Mail Server
5	ALT1.ASPMX.L.GOOGLE.COM
5	ALT2.ASPMX.L.GOOGLE.COM
10	ASPMX2.GOOGLEMAIL.COM
10	ASPMX3.GOOGLEMAIL.COM
1	ASPMX.L.GOOGLE.COM

6. Click **Save Changes**.

1. In the Barracuda Email Security Service web interface, click the link at the top of the page to start the wizard.
2. Click **Get Started**; the **Specify Primary Email Domain** page displays. Enter the primary email domain

to be filtered. You can add additional domains later.

3. Click **Next**. The **Specify Email Servers** page displays. Enter the hostname/IP address of the mail server for the entered domain. Emails will be sent to this server after being scanned by the Barracuda Email Security Service. If the servers do not pre-populate, enter the primary G Suite destination mail servers as follows:

Priority	G Suite Destination Mail Server
5	ALT1.ASPMX.L.GOOGLE.COM
5	ALT2.ASPMX.L.GOOGLE.COM
10	ASPMX2.GOOGLEMAIL.COM
10	ASPMX3.GOOGLEMAIL.COM
1	ASPMX.L.GOOGLE.COM

   After completing the setup, you must manually edit the priorities for each server from the **Domains > Domain Settings** page.

4. Enter an email address to test the server configuration, and click **Test All Mail Servers**.

5. Once the mail server is verified, the **Verified** ( ) icon displays in the **Status** column and a confirmation message displays at the top of the page.
6. Click **Next**. The **Configure Settings** page displays. Select from the following options:
   1. **Virus Protection** – Set to **On** to direct the Barracuda Email Security Service to detect and block viruses on inbound email.
   2. **Spam Protection** – Set to **On** to direct the Barracuda Email Security Service to evaluate inbound mail for spam based on a score assigned to each processed message. When set to **Off** inbound mail is not scanned for spam.

   3. **Spam Scoring** – Set **Spam Protection** to **On** to enable **Spam Scoring**. Scoring ranges from 1 (definitely not spam) to 10 (definitely spam). Setting a score of '1' will likely block legitimate messages while setting a score of '10' will allow more messages through the system. Based on this score the Barracuda Email Security Service blocks messages that appear to be spam and logs these messages in the user's Message Log with **Score** as the reason for the block.

      The following features, configured on the **Inbound Settings > Anti-Spam/Antivirus** page, are enabled when **Spam Protection** is set to **On**:
      • **Barracuda Reputation Block List (BRBL)** – Database of IP addresses manually verified to be a noted source of spam.
      • **Barracuda Real-Time System (BRTS)** – Advanced service to detect zero-hour spam and virus outbreaks even where traditional heuristics and signatures to detect such messages do not yet exist. Each quarantined message has a reason of **BRTS** in the Message Log.
      • **Sender Policy Framework (SPF)** – Block Fail is disabled.
      • **Barracuda Anti-Fraud Intelligence** – Barracuda Networks anti-phishing detection which uses a special Bayesian database for detecting Phishing scams.
      • **Intent Analysis** – Blocking based on intent analysis.
      • **CloudScan Scoring** – A cloud-based spam scanning engine which assigns a score to each message processed ranging from 0 (definitely not spam) to 10 (definitely spam).

7. Click **Next**. The **Route Email Through Barracuda** page displays.

8. To verify your domain, replace your current MX records with the Barracuda Email Security Service Primary and Backup MX records displayed on the page.

   During the evaluation period, to complete the verification process but allow your legitimate mail to continue using your current mail server, you can add the MX records with a low priority, for example, *99*.

   Some mail may appear in the Message Log after making this MX record change as spammers routinely send mail to all MX records for a domain.

   Once you have made the change to your MX records, return to the **Route Email Through Barracuda** page and click **Verify MX Records**. The Barracuda Email Security Service should see the changes made and verify your domain. If the domain does not verify correctly, verify that your MX changes are live. You can do this by using the following sites that return your MX information:

   http://mxtoolbox.com/
   https://toolbox.googleapps.com/apps/dig/ (select the MX option)

   If your domain's MX records do not display in the Barracuda Email Security Service MX records, you must wait until they display before your domain can be verified.

9. If you do not want to route your email through Barracuda Email Security, select **I do not want to route my e-mail through Barracuda at this time**, and select the verification option:

   Click here to see more

   1. **CNAME Records** – To use the CNAME records method to verify the domain ownership:

      1. Log in to your DNS Server and, under this domain, create a subdomain whose name is created by concatenating 'barracuda' and the CNAME token shown in the **Route Email Through Barracuda** page. For example:
         `barracuda30929916985.corpdomain.com`

      2. Point the CNAME record of that subdomain to ess.barracuda.com

         Allow the DNS propagation to take effect before proceeding.

      3. Click **Confirm Validation** in the **Route Email Through Barracuda** page.

   2. **Email to Technical Contact** – This method sends a verification email to the technical contact email address, if it exists, listed on your domain's WHOIS entry.

      This verification option is not available if the Barracuda Email Security Service cannot find your domain's WHOIS entry. If there is not a technical contact, then only the **MX Records**, **CNAME**, and **Email to the Postmaster** options displays on this page.

   3. **Email to the postmaster** – This method sends a verification email to the postmaster email address for your domain. The confirmation email includes a link that the recipient must click to verify the domain.

      This option is available if the Barracuda Email Security Service can find your postmaster in your

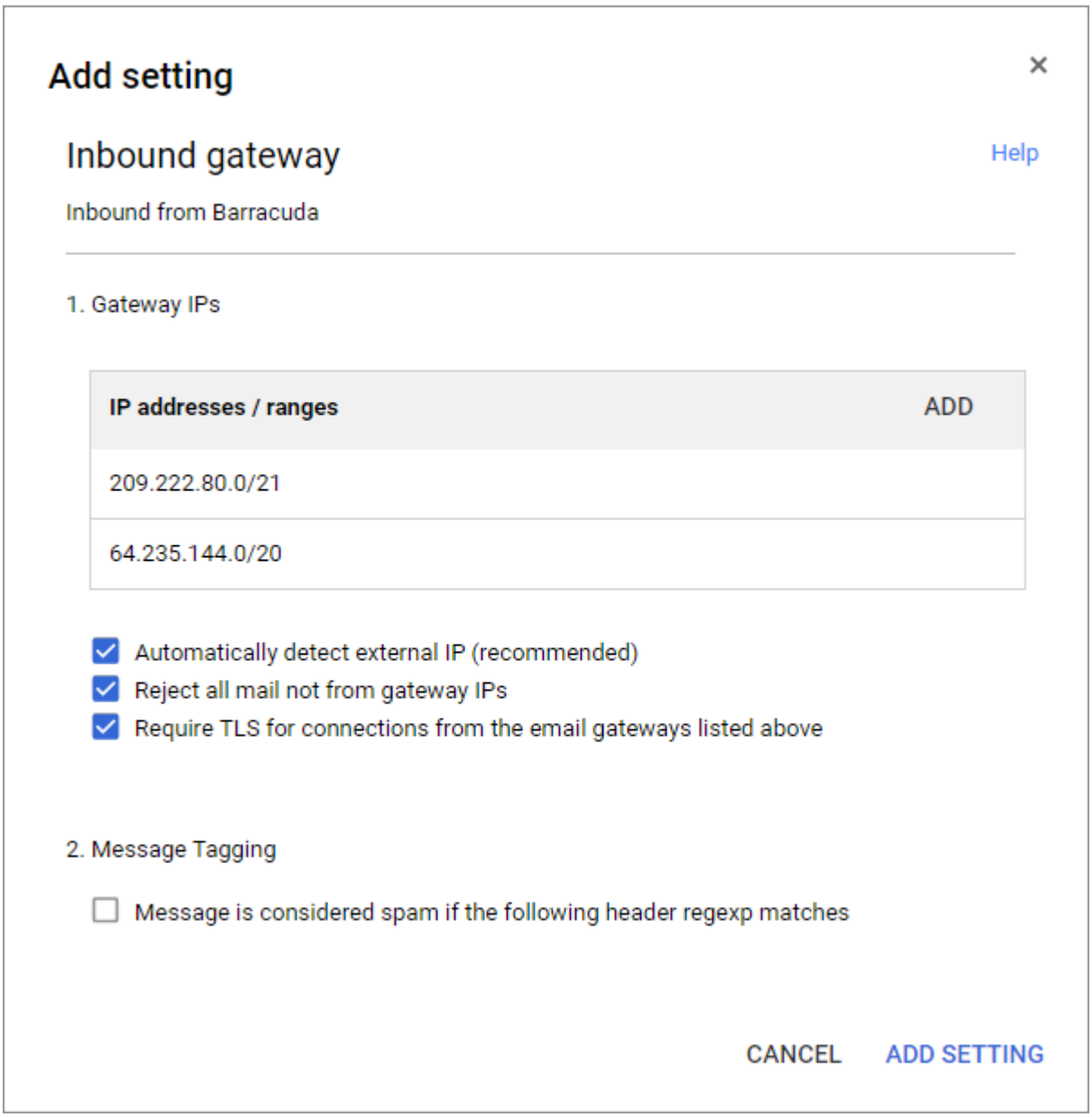
domain’s WHOIS records. This method sends a verification email to the postmaster email address for your domain. The confirmation email includes a link that the recipient must click to verify the domain.

10. Click **Next**, and click **Next** once again.
11. On the **Select Data Center Region** page, select the data center for your locale, and click **Get Started**.
12. Complete the wizard pages.
13. The **Confirmation** page displays. Confirm domain ownership, and then click **Done**.
14. Go to the **Domains** page and verify your settings.

Step 2. 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 in to the G Suite admin console at https://admin.google.com.
2. From the **Home** page, go to **Apps > G Suite > Gmail**.
3. Scroll to the bottom of the page, and click **Advanced settings**.
4. Scroll to the **Inbound gateway** section. Click **Enable**, and click **Edit**.
5. In the **IP addresses / ranges** section, type `64.235.144.0/20`, and click **ADD**.
6. Click in the **IP addresses / ranges** section again, type `209.222.80.0/21`, and click **ADD**.
7. Select the following options:
    1. **Automatically detect eternal IP (recommended)**
    2. **Reject all mail not from gateway IPs**
    3. **Require TLS for connections from the email gateways listed above**
8. In the **Message Tagging** section, clear the option **Message is considered spam if the following header regexp matches**:



9. Click **ADD SETTING**.

Step 3. Configure Sender Policy Framework for Outbound Mail

To assure Barracuda Networks is the authorized sending mail service of outbound mail from your Barracuda Email Security Service, add the following to the Sender Policy Framework (SPF) record INCLUDE line of the SPF record for your sending mail server for each domain sending outbound mail. Select the relevant SPF INCLUDE based on the region you selected for your Barracuda Email Security Service.

See Sender Authentication for more information.

For example, your record would 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 HARDFail SPF for your domain based on your Barracuda Email Security Service instance. For example: `v=spf1 include:spf.ess.barracudanetworks.com -all`

See Sender Policy Framework for Outbound Mail for INCLUDE entries based on your Barracuda Email Security Service instance.

Step 4. Configure Outbound Mail Flow (Optional)

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

1. Scroll to the **Routing** section, and locate **Outbound gateway**.
2. Enter the Outbound smart hostname provided to you in the settings for your domain within the Email Security Service interface:

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

Restrict Local Email (Optional)

By default, both internal–sending and external–sending emails are routed through the Barracuda Email Security Service.

If you do not want to send internal email to Barracuda Email Security Service, complete the following steps:

1. Sign in to the G Suite domain console. In the left pane, click **Apps**. In the **Apps Settings** page, click **G Suite**, and then click **Gmail > Advanced settings**.
2. Click the **Hosts** tab, and click **Add Route**. In the **Name** field type a name to represent the new host, for example, type: `Local Email`
3. In the **Host name or IP address**, type Google's primary destination hostname: `ASPMX.L.GOOGLE.COM`
4. In the **Port** field, type: 25
5. Click the **General Settings** tab. In the **Routing** section, scroll down to **Routing**, and click **Configure**.
6. In the **Messages to affect** section, select **Internal - sending**
7. Scroll down to **Route**, and select **Change route**. From the drop-down menu, select the new host created above in step 6, in this example, **Local Email**, and click **Add Setting**.

Step 5. Enable Advanced Threat Protection

Files blocked by Advanced Threat Protection (ATP) display on the **Dashboard**.

1. Go to the **ATP Settings** tab, and select the desired option in the **Enable Advanced Threat Protection** section:
   - **Deliver First, then Scan** – Attachments are delivered with the message to the recipient and then scanned by the ATP service; if a virus is detected, an email notification is sent to the email recipient. Additionally, if **Notify Admin** is set to **Yes**, and a virus is detected in the scanned

attachment, an email is sent to the administrator.
    - **Scan First, then Deliver** – Attachments are scanned by the ATP service before delivery. If a virus is detected in the attachment the message is blocked, otherwise it is delivered to the recipient.
2. Select whether to **Notify Admin** if a virus is detected in a scanned attachment. When set to **Yes**, enter the **ATP Notification Email** address in the associated field.

When ATP is set to either **Deliver First, then Scan** or **Scan First, then Deliver**, you can exempt sender email addresses, sender domains, recipient email addresses, recipient domains, or sender IP addresses from ATP scanning in the **ATP Exemptions** section on the **ATP Settings** page.

For more information on ATP, refer to the following articles:

- Understanding Advanced Threat Protection
- Advanced Threat Protection Sample Email Notifications
- Advanced Threat Protection Reports

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

Figures