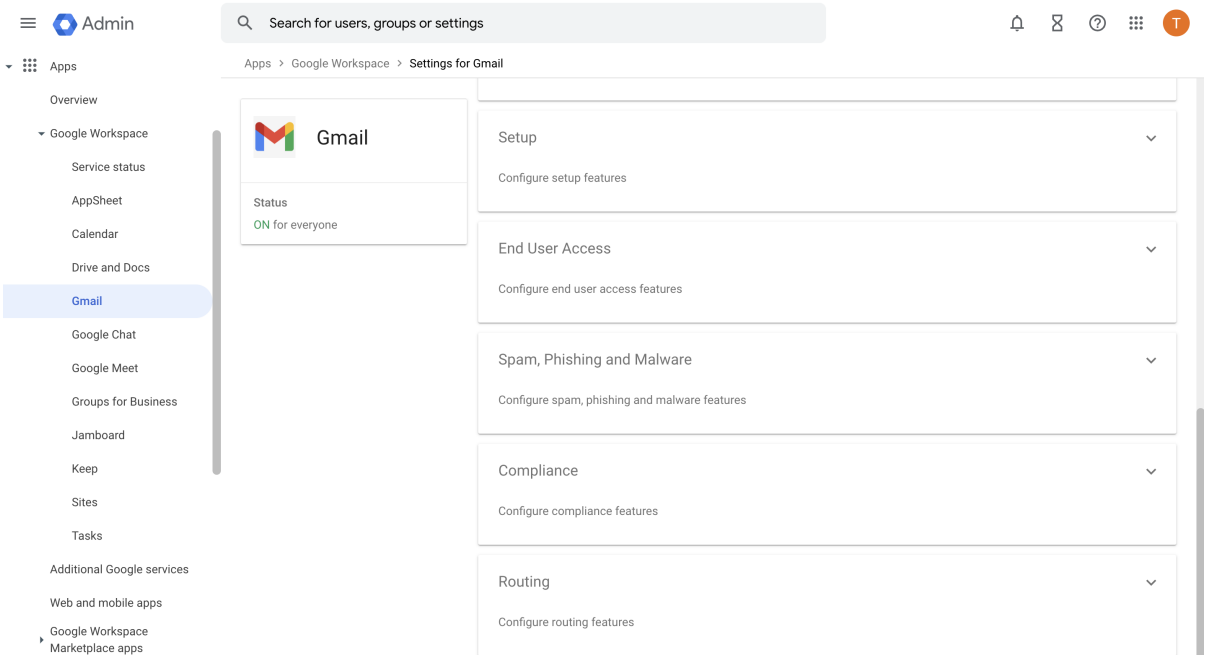
How to Configure Google Workspace for Inbound and Outbound Mail

https://campus.barracuda.com/doc/3421/

This article addresses configuring Google Workspace Business and Education editions with the Barracuda Email Security Gateway as your inbound and/or outbound mail gateway.

Inbound Configuration

1. Log into the Google Workspace admin console at https://admin.google.com.
2. From the **Home** page, go to **Apps > Google Workspace > Gmail.** From the **Home** page, go to **Apps > Google Workspace > Gmail > Spam, Phishing, and Malware.**



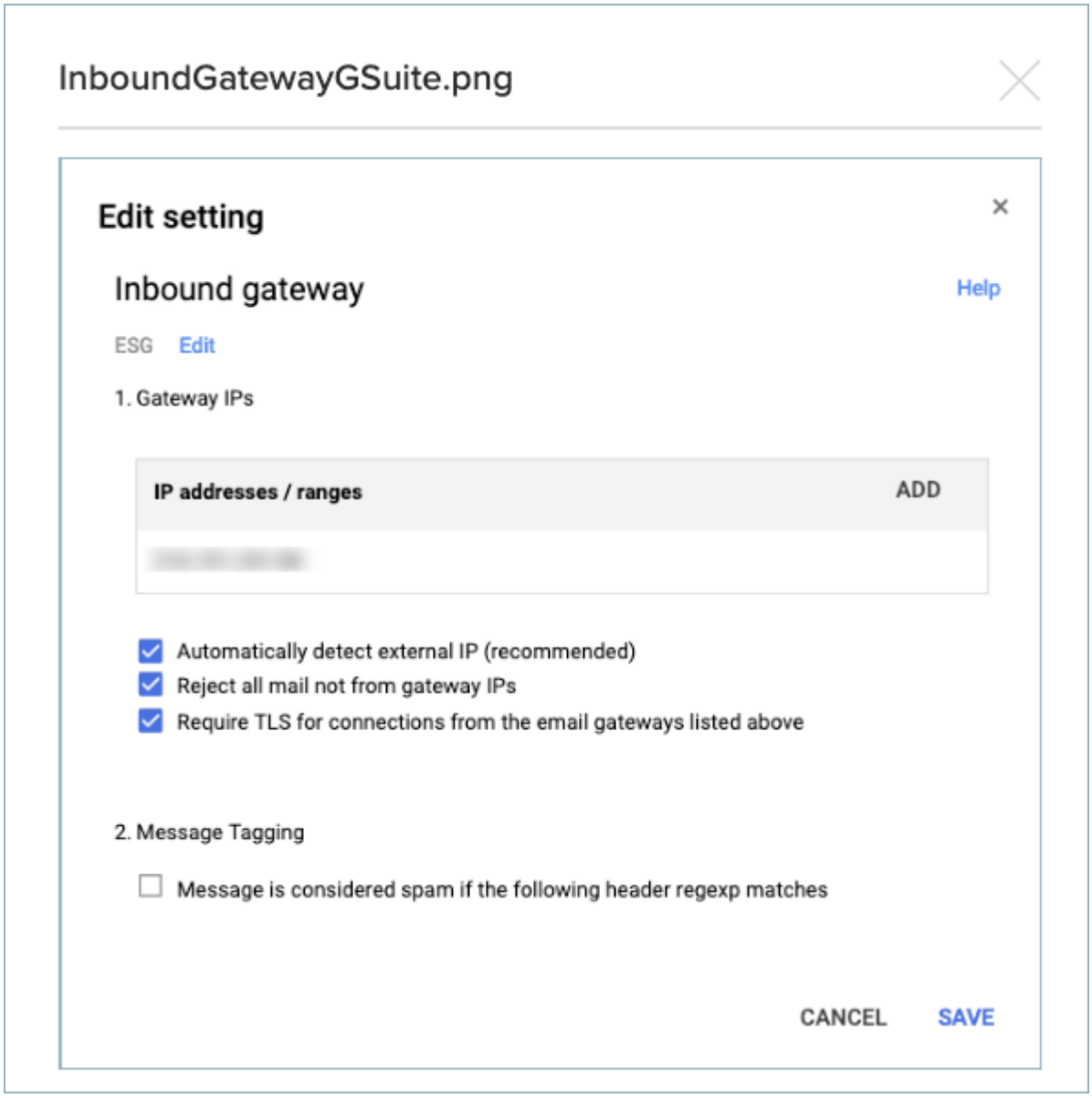
3. Scroll to the **Inbound gateway** section and, on the right, click **Enable**, and then click **Edit**.
4. In the **Gateway IPs** section, under **IP Addresses / Ranges**, enter the public IP addresses of the Barracuda Spam Email Security Gateway(s), specifying either a block of addresses or individual IP addresses.
5. Select the following options:
    1. **Automatically detect external IP (recommended)**
    2. **Reject all mail not from gateway IPs.** MAKE SURE TO CHECK THIS BOX. All other mail

will be rejected.

3. **Require TLS for connections from the email gateways listed above**

6. Click **Save**.
   More information on inbound gateways can be found here.

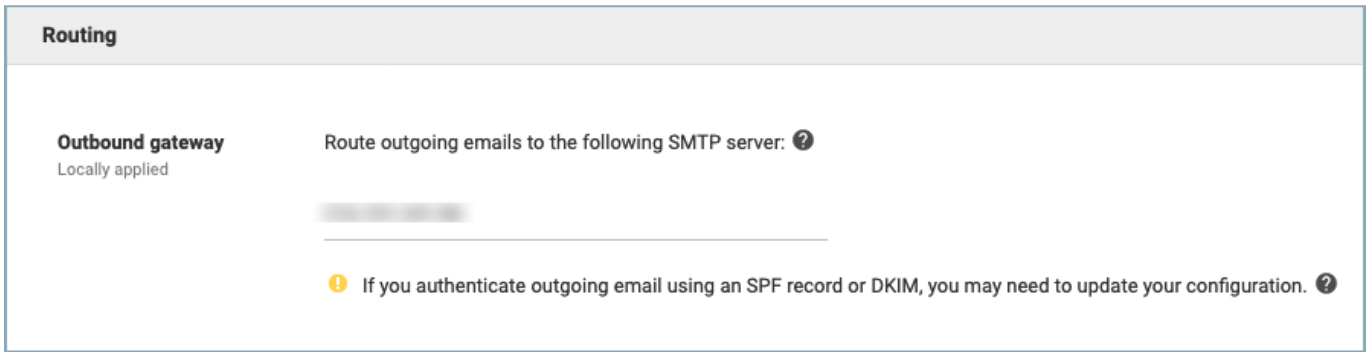
Figure 1: Google Workspace - Inbound Gateway Settings



Outbound Configuration

1. Scroll to the Routing section, and locate **Outbound gateway**.
2. Enter the IP address of the Barracuda Email Security Gateway that is the outbound mail gateway.

Figure 2: Google Workspace - Outbound Gateway Settings



More information about outbound gateways can be found here.

> Google Workspace IP Addresses can change, so please refer to this Google documentation.

Additional settings:

- nslookup -q=TXT _netblocks.google.com 8.8.8.8
- server: google-public-dns-a.google.com
- address: 8.8.8.8
- Non-authoritative answer:

_netblocks.google.com text ="v=spf1 ip4:216.239.32.0/19ip4:64.233.160.0/19ip4:66.249.80.0/20

ip4:72.14.192.0/18ip4:209.85.128.0/17ip4:66.102.0.0/20ip4:74.125.0.0/16
ip4:64.18.0.0/20ip4:207.126.144.0/20ip4:173.194.0.0/16 ?all"

Configuring the Barracuda Email Security Gateway

1. Navigate to **DOMAINS > Domain Manager** and specify your domain in **New Domain Name**, then click **Add Domain**.
2. Click the Manage Domain link and then **BASIC > IP Configuration.** Add the Google Workspace destination mail servers as follows:

Priority	Value/Answer/Destination
1	ASPMX.L.GOOGLE.COM
5	ALT1.ASPMX.L.GOOGLE.COM
5	ALT2.ASPMX.L.GOOGLE.COM
10	ALT3.ASPMX.L.GOOGLE.COM

10	ALT4.ASPMX.L.GOOGLE.COM

Also add the **Destination Server** name/IP address or hostname that receives email after spam and virus scans. It is usually best to use a hostname rather than an IP address so that the destination mail server can be moved and DNS updated at any time without having to make changes to the Barracuda Email Security Gateway configuration.

If you set **Use MX Records** (on the same page) to *Yes*, you must enter a domain name for this field. If multiple servers are specified, then the delimiter used determines the behavior (see below). Note that you can either configure **Use MX Records** for *all* domains from the **BASIC > IP Configuration** page, or you can configure it per-domain from **DOMAINS > Domain Manager > Manage Domains,** then using the **BASIC > IP Configuration** page for the domain you choose to manage. It is *NOT* recommended to set **Use MX Records** to *Yes* to avoid a potential mail loop.

1. **Comma** (",") or semi-colon (";") - Each entry in the list will used in round-robin fashion, with relative weights determined by the number of times a particular entry is listed.
2. **Space** (" ") - Each entry in the list will be treated as a failover list, with an entry being used only if all entries preceding it in the list are unreachable.

For more information about what it means to use MX records, please see Using MX Records.

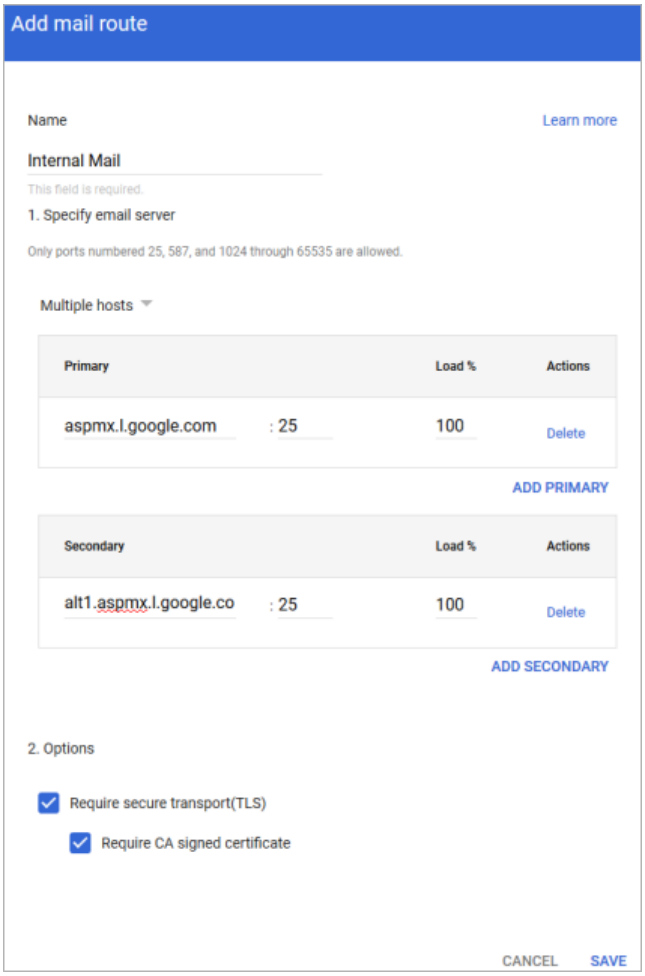
How to Configure Google Workspace to Bypass the Barracuda Email Security Gateway for Internal Mail

To ensure that your internal mail stays internal, you must create a routing rule. Here are the instructions:

Step 1. Create Local Host

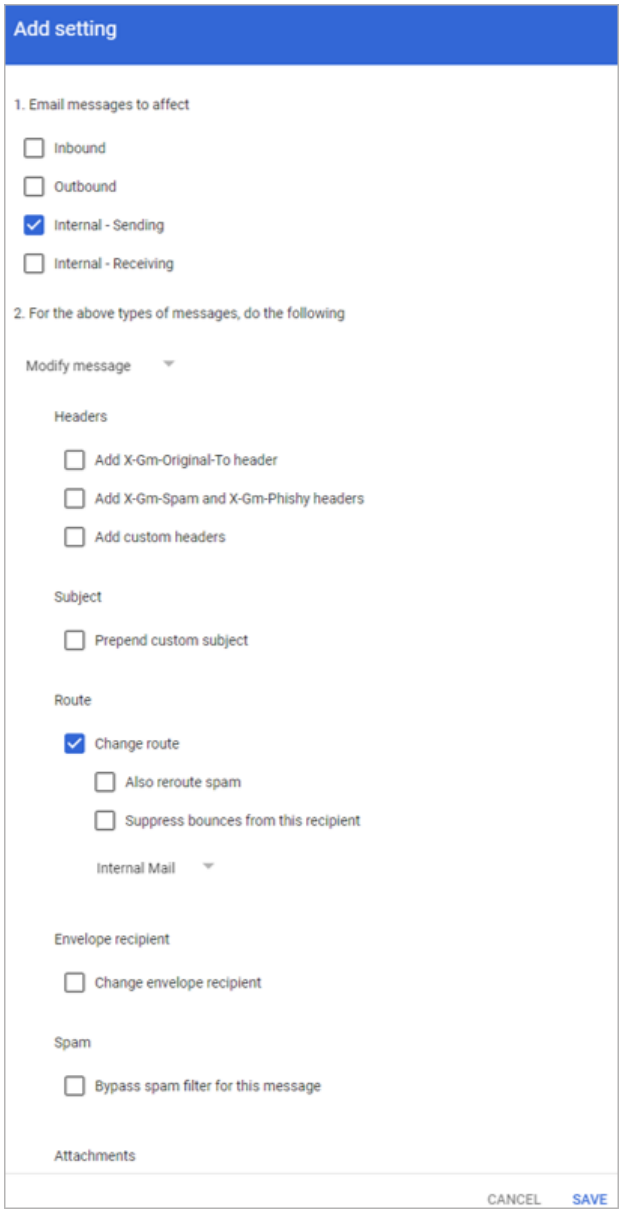
1. Log into the Google Workspace admin console at https://admin.google.com.
2. From the **Home** page, go to **Apps > Google Workspace > Gmail**.
3. Click **Hosts**.
4. Click **Add Route**. Enter a route name. For example, "Internal Mail".
5. Select **Multiple hosts**.
6. Enter the following **Primary 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**.

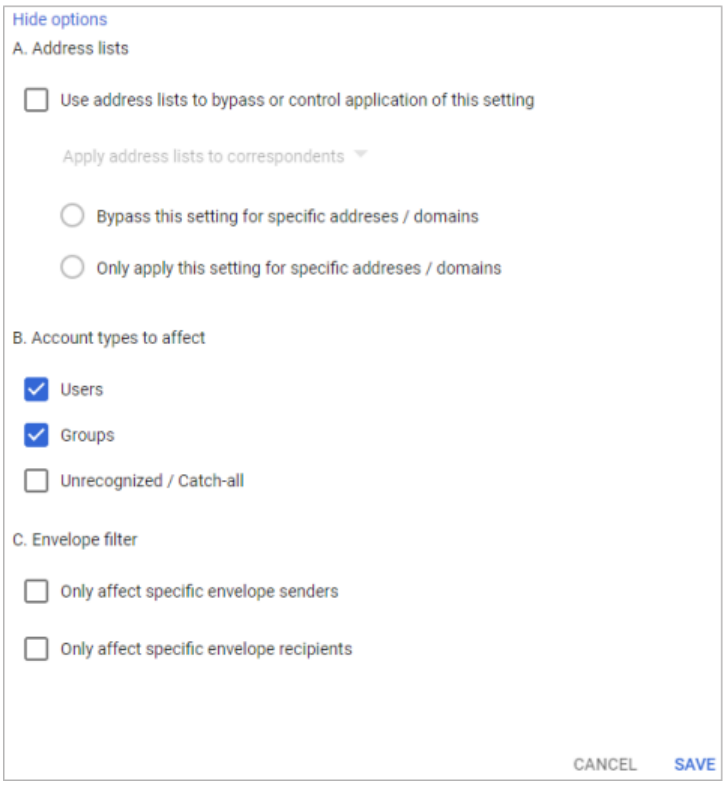


Step 2. Create Routing Rule

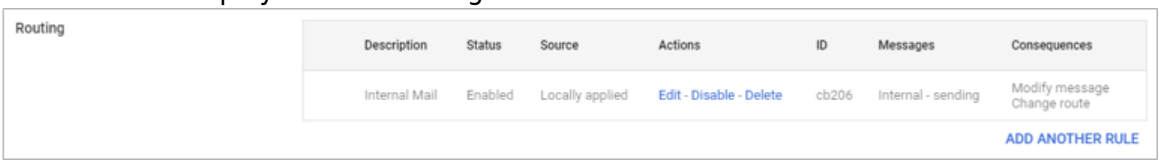
1. Navigate to **Apps > Google Workspace > Gmail**.
2. Click **Routing** at the bottom of the page.
3. Under the **Routing** section, click **Configure**.
4. Enter a name for the rule. For example, "Internal Mail".
5. Under **Email messages to affect**, select **Internal - Sending**.
6. Under For the 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.



Now all internal mail is routed directly to Google servers, and all other mail routes through Outbound Gateway.

Figures

1. InboundConfig1.png
2. gateway-ips.png
3. OutboundGatewayGSuite.png
4. addInternalMail1.png
5. addRoutingRule1a.png
6. addRoutingRule1b.png
7. newRule1.png