

Step 2 - Configure Google Workspace for Inbound and Outbound Mail

<https://campus.barracuda.com/doc/96022748/>

To deploy Email Gateway Defense with Google Workspace, you must have a Google Workspace Basic, Business, or Enterprise account. The G Suite legacy free edition is no longer available and is missing key features required for this deployment. For details on upgrading your Google Workspace subscription, refer to the Google Support article [Upgrade from G Suite legacy free edition](#).

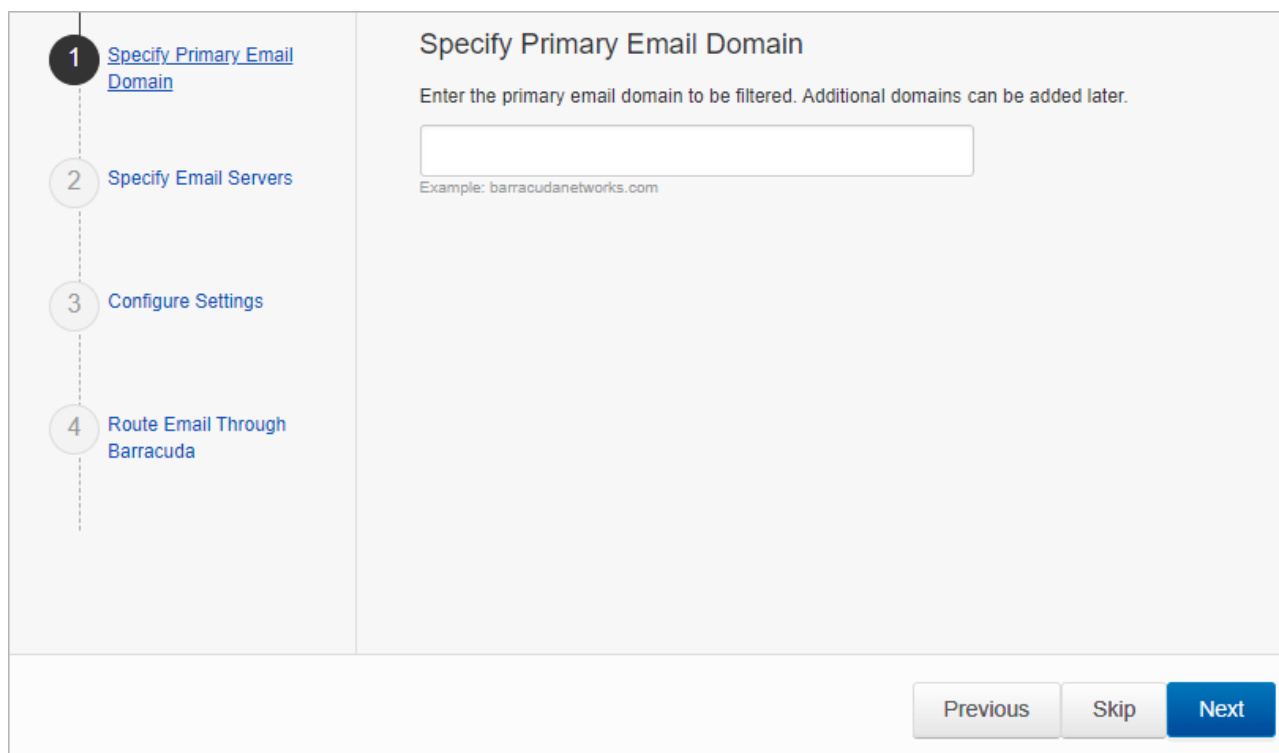
[Google IP addresses](#) and user interfaces can change; refer to the [Google Workspace Administrator Help Center](#) for updates and configuration details.

You can specify Email Gateway Defense as an *inbound mail gateway* through which all incoming mail for your domain is filtered before reaching your Google account. Email Gateway Defense 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 Email Gateway Defense 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, Email Gateway Defense 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 Email Gateway Defense (the gateway server).

Step 1. Launch the Email Gateway Defense Setup Wizard

1. Log into your Barracuda Cloud Control account. On the left side, select **Email Gateway Defense**.
The Email Gateway Defense 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 Email Gateway Defense. Then click **Next**.



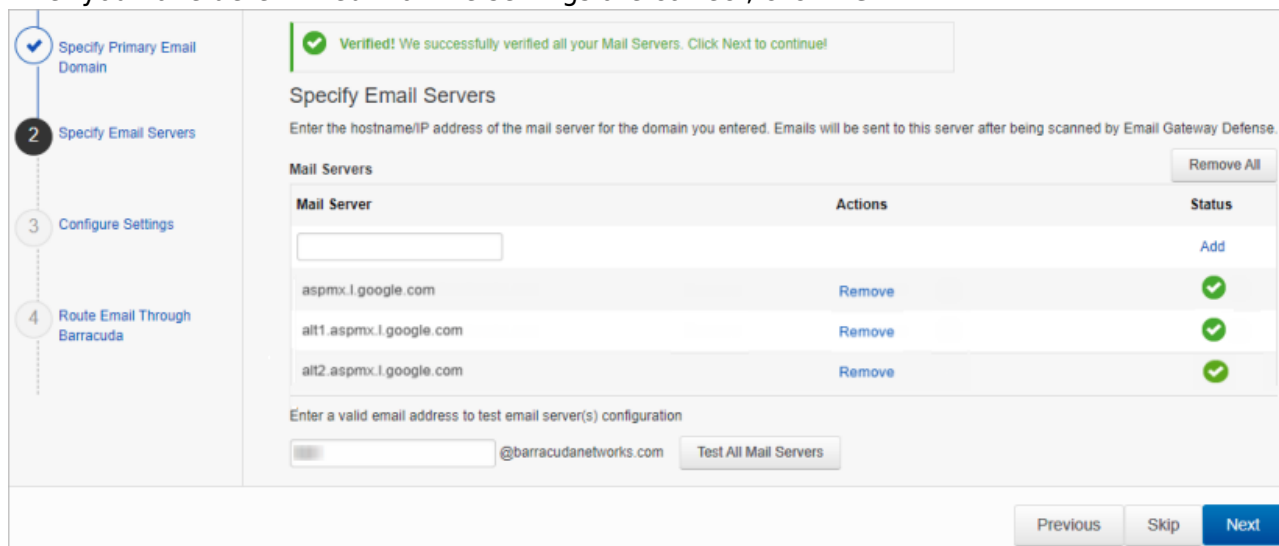
The screenshot shows the first step of the setup wizard, 'Specify Primary Email Domain'. On the left, a vertical progress bar has four steps: 1. Specify Primary Email Domain (selected), 2. Specify Email Servers, 3. Configure Settings, and 4. Route Email Through Barracuda. The main content area has the title 'Specify Primary Email Domain' and a subtitle 'Enter the primary email domain to be filtered. Additional domains can be added later.' Below this is a text input field with the example 'barracudanetworks.com' shown underneath. At the bottom right, there are three buttons: 'Previous' (disabled), 'Skip' (disabled), and 'Next' (active).

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**.



The screenshot shows the second step of the setup wizard, 'Specify Email Servers'. The progress bar on the left now has step 2 selected. The main content area has a green success message: 'Verified! We successfully verified all your Mail Servers. Click Next to continue!'. Below this is the title 'Specify Email Servers' and a subtitle 'Enter the hostname/IP address of the mail server for the domain you entered. Emails will be sent to this server after being scanned by Email Gateway Defense.' There is a 'Mail Servers' section with a table. The table has three columns: 'Mail Server', 'Actions', and 'Status'. It lists three servers: 'aspmx.l.google.com', 'alt1.aspmx.l.google.com', and 'alt2.aspmx.l.google.com', each with a 'Remove' link and a green checkmark status. There is an 'Add' button at the bottom right of the table. Below the table, there is a text input field for 'Enter a valid email address to test email server(s) configuration' with the example '@barracudanetworks.com' and a 'Test All Mail Servers' button. At the bottom right, there are three buttons: 'Previous' (disabled), 'Skip' (disabled), and 'Next' (active).

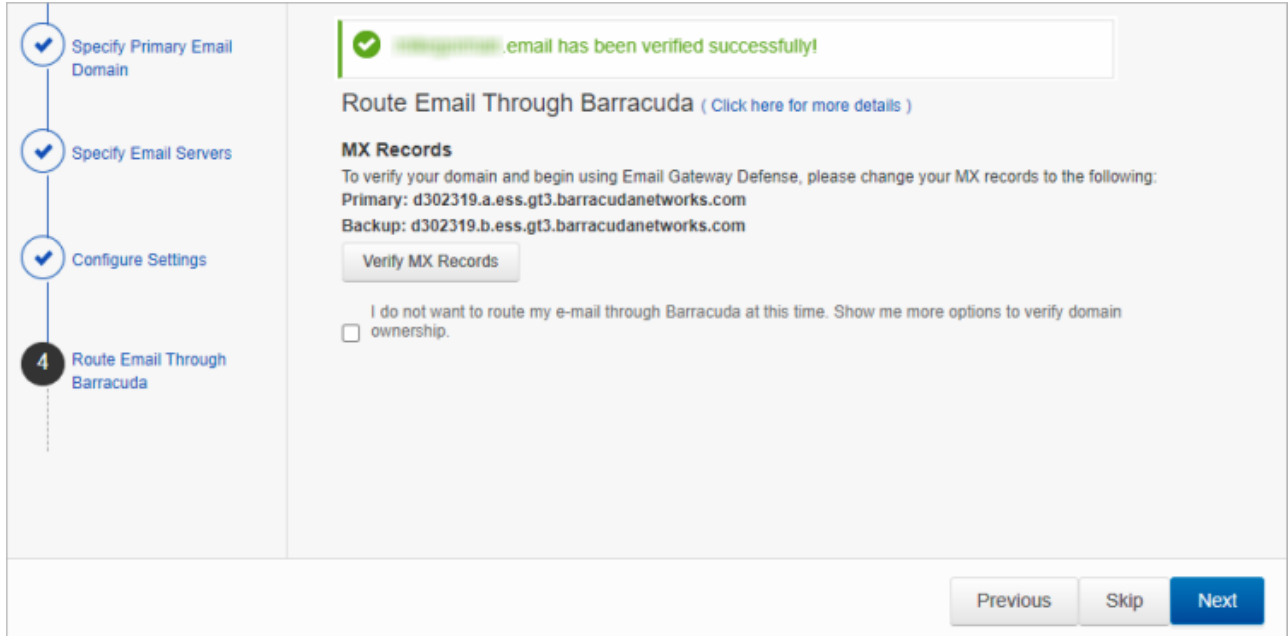
5. Select your settings, accepting the default values or making changes if needed, then click **Next**.
6. Barracuda Networks recommends verifying your domain via MX records with Priority 99. If you do not want to update MX records now, check the box and select a different method.

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 Email

Gateway Defense customer will be processed normally by your Email Gateway Defense 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.

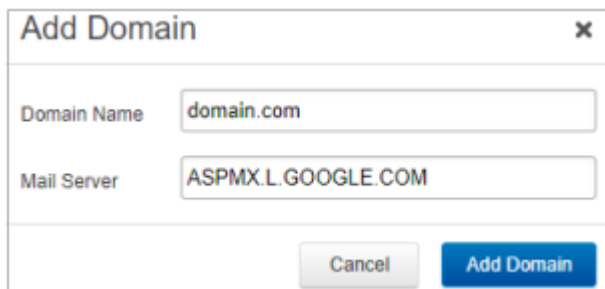
8. Click **Finish** to finalize the setup and close the wizard.

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 Email Gateway Defense. 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 Gateway Defense**. Select the **Domains** tab, then click **Add Domain**.
2. Enter the domain name and the Primary MX record for Google: (see Table 1 below).

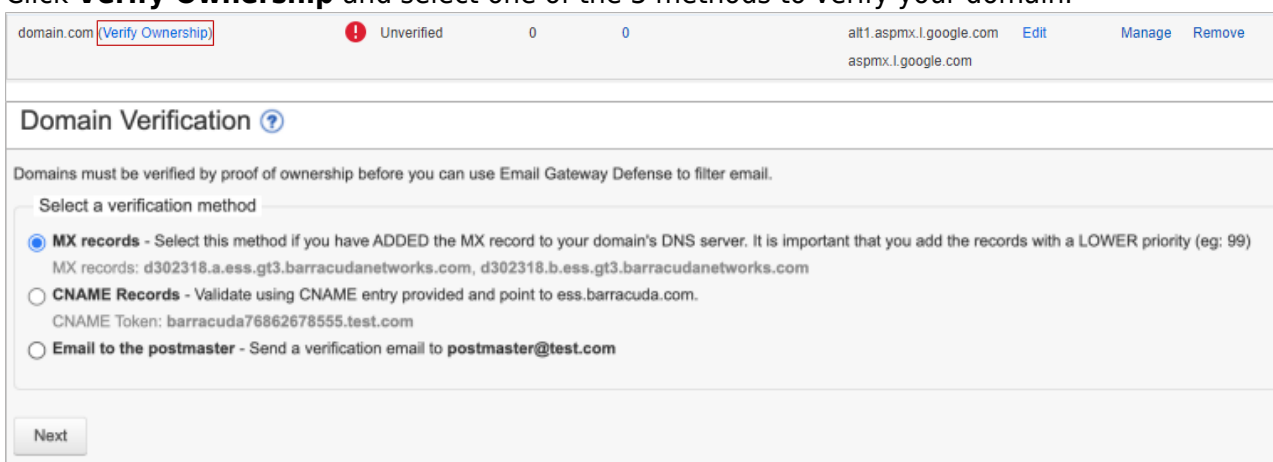



Add Domain [X]

Domain Name:

Mail Server:

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.



domain.com [Verify Ownership](#)  Unverified 0 0 alt1.aspmx.l.google.com Edit Manage Remove aspmx.l.google.com

Domain Verification ?

Domains must be verified by proof of ownership before you can use Email Gateway Defense to filter email.

Select a verification method

☒ **MX records** - Select this method if you have ADDED the MX record to your domain's DNS server. It is important that you add the records with a LOWER priority (eg: 99)
 MX records: d302318.a.ess.gt3.barracudanetworks.com, d302318.b.ess.gt3.barracudanetworks.com

☐ **CNAME Records** - Validate using CNAME entry provided and point to ess.barracuda.com.
 CNAME Token: barracuda76862678555.test.com

☐ **Email to the postmaster** - Send a verification email to **postmaster@test.com**


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. Google Workspace Destination Mail Servers

Priority	Google Workspace 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 Email Gateway Defense MX records; otherwise mail delivery issues may be introduced.

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. 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 Networks IP ranges.

5. Click **Add** under **Gateway IPs**.

6. Enter the IP address/range for your Barracuda Networks region.

For example, if you are in the US region, type 209.222.80.0/21, click **Save**. For other regions, refer to the IP addresses listed in [Email Gateway Defense IP Ranges](#).

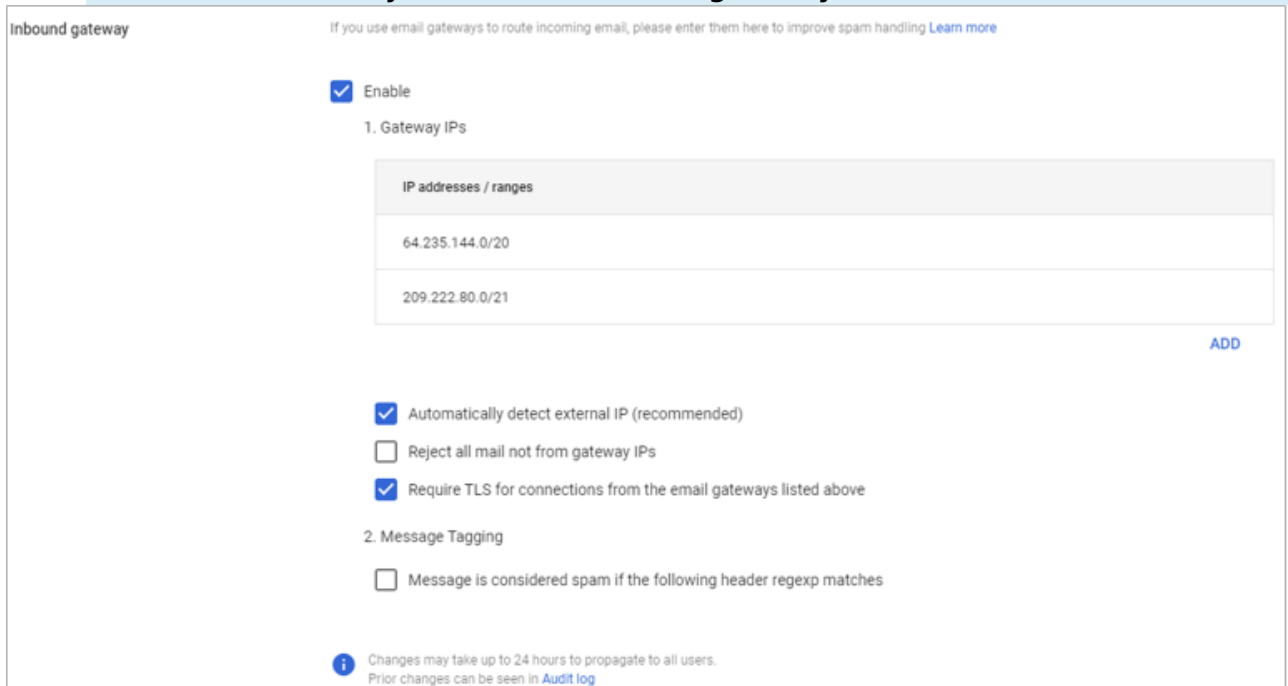
To add another IP address/range, click **Add** and type in the IP address/range. Click **Save** again.

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 Networks (default), you must also select **Reject all mail not from gateway IPs**.



Inbound gateway

If you use email gateways to route incoming email, please enter them here to improve spam handling [Learn more](#)

☒ Enable

1. Gateway IPs

IP addresses / ranges
64.235.144.0/20
209.222.80.0/21

[ADD](#)

☒ Automatically detect external IP (recommended)

☐ Reject all mail not from gateway IPs

☒ Require TLS for connections from the email gateways listed above

2. Message Tagging

☐ Message is considered spam if the following header regexp matches

Changes may take up to 24 hours to propagate to all users. Prior changes can be seen in [Audit log](#)

8. Click **Save**.

Step 4. Internal Mail

By default, your internal mail is sent out to your inbound MX record, which points to Email Gateway Defense. 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 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**.

Add mail route

Name [Learn more](#)

Internal Mail
This field is required.

1. Specify email server
Only ports numbered 25, 587, and 1024 through 65535 are allowed.

Multiple hosts ▼

Primary		Load %	Actions
aspmx.l.google.com	: 25	100	Delete

[ADD PRIMARY](#)

Secondary		Load %	Actions
alt1.aspmx.l.google.co	: 25	100	Delete

[ADD SECONDARY](#)

2. Options
☒ Require secure transport(TLS)
☒ Require CA signed certificate

[CANCEL](#) [SAVE](#)

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*.

Add setting

1. Email messages to affect

☐ Inbound

☐ Outbound

☒ Internal - Sending

☐ Internal - Receiving

2. For the above types of messages, do the following

Modify message ▾

Headers

☐ Add X-Gm-Original-To header

☐ Add X-Gm-Spam and X-Gm-Phishy headers

☐ Add custom headers

Subject

☐ Prepend custom subject

Route

☒ Change route

☐ Also reroute spam

☐ Suppress bounces from this recipient

Internal Mail ▾

Envelope recipient

☐ Change envelope recipient

Spam

☐ Bypass spam filter for this message

Attachments

[CANCEL](#) [SAVE](#)

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

[Hide options](#)

A. Address lists

☐ Use address lists to bypass or control application of this setting

Apply address lists to correspondents ▼

☐ Bypass this setting for specific addresses / domains

☐ Only apply this setting for specific addresses / domains

B. Account types to affect

☒ Users

☒ Groups

☐ Unrecognized / Catch-all

C. Envelope filter

☐ Only affect specific envelope senders

☐ Only affect specific envelope recipients

[CANCEL](#) [SAVE](#)

8. Click **Save**.

The new rule displays in the Routing section.

Routing

Description	Status	Source	Actions	ID	Messages	Consequences
Internal Mail	Enabled	Locally applied	Edit - Disable - Delete	cb206	Internal - sending	Modify message Change route

[ADD ANOTHER RULE](#)

Step 5. Configure Sender Policy Framework for Outbound Mail

To ensure Barracuda Networks is the authorized sending mail service of outbound mail from Email Gateway Defense, 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 Networks 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 Networks 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 Networks instance. For example: `v=spf1 include:spf.ess.barracudanetworks.com -all`

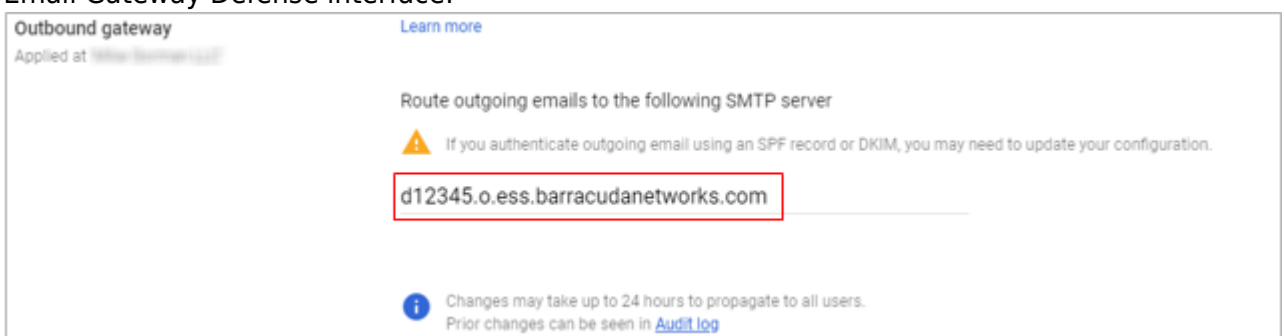
For more information, see [Sender Authentication](#).

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 [Google Workspace 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 Email Gateway Defense interface:



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

Figures

1. egd_primaryDomain.png
2. egd_gsuiteEmailServers1a.png
3. egd_verifySuccess.png
4. addDomainGsuite.png
5. verifyOwnershipGsuite.png
6. domainVerificationGsuite.png
7. verify_Icon.png
8. addRoutingRule2a.png
9. addInternalMail1.png
10. addRoutingRule1a.png
11. addRoutingRule1b.png
12. newRule1.png
13. outboundGateway1a.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.