How to Configure Sender Policy Framework

https://campus.barracuda.com/doc/96022990/

If you make setting changes, allow a few minutes for the changes to take effect.

Use the steps in this article to configure Sender Policy Framework (SPF) checking for Email Gateway Defense.

Important
If you have SPF checking enabled on your mail server or network, it is critical when using Email Gateway Defense that you either disable SPF checking in the service or add the Email Gateway Defense IP ranges to your SPF exemptions based on your Barracuda Networks instance; see Email Gateway Defense IP Ranges Used for Configuration for a list of IP rages based on your Barracuda Networks instance.

Otherwise, your SPF checker blocks mail from domains with an SPF record set to **Block** because the mail is coming from an Email Gateway Defense Service IP address not in the sender's SPF record.

Configure SPF for Inbound Mail

1. Log into your Barracuda Cloud Control account, and click **Email Gateway Defense** in the left pane.
2. Go to the **Inbound Settings > Sender Authentication** page, and select from the available options in the **Enable Sender Policy Framework Checking** section:
   - **Hard Fail** – Response indicates that the message sender's IP address does not match the IP address or range of IP addresses specified in the sending domain name's SPF record, and that the real owner of the domain has specifically indicated that such messages should be rejected (blocked) as spoofed.
     - **Block** – Messages from a domain that fails SPF checking are blocked.
     - **Quarantine** – Messages from a domain that fails SPF checking are quarantined.
     - **Off** – When set to Off, Email Gateway Defense does not query DNS for an SPF record for the sending domain to verify whether the sender is the true owner of that domain. This is the default setting.
   - **Soft Fail** – Response indicates that the message sender's IP address does not match the IP address or range of IP addresses specified in the sending domain name's SPF record, and that the domain owner did not specify how the message should be handled.
     - **Block** – Messages from a domain that fails SPF checking are blocked.
     - **Quarantine** – Messages from a domain that fails SPF checking are quarantined.

- **Off** – When set to Off, Email Gateway Defense does not query DNS for an SPF record for the sending domain to verify whether the sender is the true owner of that domain. This is the default setting.

When Hard Fail is set to **Off**, Soft Fail options are disabled.

You can optionally enable Sender Rewriting Scheme (SRS) for a specific domain on the **Domains > Domain Settings** page. When enabled, the sending mail server IP address is visible to the SPF verification agent on the recipient's end. The recipient's SPF agent checks the reverse MX records for your domain and verifies your IP address as an authorized sender to ensure message delivery to the recipient.

3. Click **Save Changes**.

When **Enable Sender Policy Framework Checking** is set to **Off**, Email Gateway Defense does not query DNS for an SPF record for the sending domain to verify whether the sender is the true owner of that domain. If you are concerned about domain spoofing, enable one of the SPF options.

Exempt Trusted IP Addresses and Domains from SPF Checks

You can exempt mail relay servers and other machines from SPF checks. Mail from these IP addresses and domains is still scanned for spam.

1. Log into your Barracuda Cloud Control account, and click **Email Gateway Defense** in the left pane.
2. Go to the **Inbound Settings > Sender Authentication** page, and in the **Enable Sender Policy Framework Checking** section, use one or both of the following:
   - **SPF Exemptions by IP Address** – Enter the **IP Address** and **Netmask** and optional **Comment**.
   - **SPF Exemptions by Domain** – Enter the **Domain** and optional **Comment**.

     Note: Usage requires exact matching after the @ sign. For example, `domain.com` will not work for `sub.domain.com`. You must create a separate entry for `sub.domain.com`.

   Alternatively, use the **Bulk Edit** button. **Note** that the maximum number of entries that can be added for this policy is 2500.
3. Click **Add** in the **Actions** column, and click **Save Changes**.

Block on No SPF Records

You can configure what happens when senders send mail from or through mail servers whose domains lack an SPF record.

1. Log into your Barracuda Cloud Control account, and click **Email Gateway Defense** in the left pane.

2. Go to the **Inbound Settings > Sender Authentication** page, and select one of the following in the **Block on No SPF Records** section:
   - **Block** – If a sending domain does not have an SPF record, the mail server is blocked and mail is not delivered to the user.
   - **Quarantine** – If a sending domain does not have an SPF record, mail is quarantined.
   - **Off** – When set to Off, there is no query for any senders. This is the default setting.
3. Click **Save Changes**.

Additionally, if you have known/trusted contacts that send email from or through mail servers whose domains have no SPF records, you can create exemptions for these senders to allow their mail through while still blocking mail from other mail servers that do not have SPF records.

> Note that **Block on No SPF Records** set to **Block** takes precedence over DMARC.

Configure SPF for Outbound Mail

To assure outbound mail from Email Gateway Defense that Barracuda Networks is the authorized sending mail service, add the following to the SPF record INCLUDE line for each domain sending outbound mail based on your Barracuda Networks instance.

For more information, see Email Gateway Defense Outbound IP Ranges.

AU (Australia)

```
include:spf.ess.au.barracudanetworks.com -all
```

CA (Canada)

```
include:spf.ess.ca.barracudanetworks.com -all
```

DE (Germany)

```
include:spf.ess.de.barracudanetworks.com -all
```

IN (India)

```
include:spf.ess.in.barracudanetworks.com -all
```

UK (United Kingdom)

```
include:spf.ess.uk.barracudanetworks.com -all
```

US (United States)

```
include:spf.ess.barracudanetworks.com -all
```