How to Configure Sender Policy Framework

https://campus.barracuda.com/doc/3211267/

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 the Barracuda Email Security Service.

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

Otherwise, your SPF checker blocks mail from domains with an SPF record set to **Block** because the mail is coming from a Barracuda Email Security Service IP address not in the sender's SPF record. For more information, see the Sender Policy Framework Project Overview.

Configure SPF for Inbound Mail

1. Log in to your Barracuda Cloud Control account, and click **Email Security** in the left pane.
2. Go to the **Inbound Settings > Sender Authentication** page, and select from the available options in the **Use Sender Policy Framework** section:
   - **Block FAIL** – The SPF FAIL (also referred to as Hard FAIL) response indicates that the IP address of the message sender 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 FAIL, SOFTFAIL** – The SPF SOFTFAIL 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. A SOFTFAIL means that the domain owner did not specify how such messages should be handled. Selecting this option means that messages in either the SPF SOFTFAIL or FAIL state are blocked.
   - **Off** – When set to **Off**, the Barracuda Email Security Service 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.

     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 **Use Sender Policy Framework** is set to **Off**, the Barracuda Email Security Services 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 from SPF Checks

You can exempt mail relay servers and other machines from SPF checks that are set up specifically to forward mail to the Barracuda Email Security Service from outside sources. Mail from these IP addresses is still scanned for spam.

1. Log in to your Barracuda Cloud Control account, and click **Email Security** in the left pane.
2. Go to the **Inbound Settings > Sender Authentication** page, and in the **Sender Policy Framework** section, enter the **IP Address** and **Netmask** and optional **Comment**.
3. Click **Add** in the **Actions** column, and click **Save Changes**.

Configure SPF for Outbound Mail

To assure outbound mail from your Barracuda Email Security Service 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 Email Security Service instance. For example, type: `include:spf.ess.barracudanetworks.com -all`

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