Sender Authentication

https://campus.barracuda.com/doc/3211297/

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

Sender Authentication mechanisms enable the Barracuda Email Security Service to protect your network and users from spammers who might "spoof" a domain or otherwise hide the identity of the true sender. This article describes the techniques used to verify the "from" address of a message.

Sender Policy Framework

If you have Sender Policy Framework (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 addresses based on your Barracuda Email Security Service instance.

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

SPF is an open standard specifying a method to prevent sender address forgery. The current version of SPF protects the envelope sender address, which is used for message delivery. SPF works by having domains publish reverse MX records to display which machines are designated as mail sending machines for that domain. When receiving a message from a domain, the recipient can check those records to verify mail is coming from a designated sending machine. If the message fails the SPF check, it is assumed to be spam.

Messages that fail SPF check can be blocked and are logged as such. Enable or disable the SPF feature for checking inbound mail from the **Inbound Settings > Sender Authentication** page. To configure, see How to Configure Sender Policy Framework.

Note that if you enable SPF, you may want to enable the **Sender Rewriting Scheme (SRS)**. This option is configurable from the **Advanced Configuration** section of the **Domains > Domain Settings** page and, if enabled, the Barracuda Email Security Service makes the IP address of your sending mail server visible to the agent performing SPF verification on the recipient's end.

Block on No PTR Records

While the A record for a domain points to an IP address, the PTR record resolves an IP address to a domain/hostname and is used for reverse DNS lookup.

When **Block on No PTR Records** is set to **Yes**, and a a sending domain does not have a PTR record, the mail server is blocked and the mail is not delivered to the user. When set to **No**, there is no query for any senders.

Configure on the **Inbound Settings > Sender Authentication** page.

Custom Policies

For inbound email, organizations can define their own allowed sender domains, users, or email addresses for sender authentication using the **Inbound Settings > Sender Policies** page. However, the safest way to indicate valid senders on the Barracuda Email Security Service is to exempt the IP addresses of trusted email servers from being scanned on the **Inbound Settings > IP Address Policies** page, then blocklist (block) their domain names on the **Inbound Settings > Sender Policies** page to prevent domain name spoofing.

Sender Spoof Protection

Enable Sender Spoof Protection on the **Domain Settings** page when you do not have an SPF record set up for your domain. To navigate to the **Domain Settings** page, select the **Domains** tab, then for the appropriate domain, click **Edit**. Under **Options**, locate **Enable Sender Spoof Protection**.

Use Sender Spoof Protection to block "From" addresses that use your domain. Note that Sender Spoof Protection is for inbound mail only, and does not stop your domain from being spoofed at other mail servers.

See Understanding the Domains Page for more information.