Sender Authentication

https://campus.barracuda.com/doc/16905/

Sender authentication verifies that email originates from authorized sources and helps prevent spoofing and phishing attacks. Email Gateway Defense supports **SPF**, **DKIM**, and **DMARC**, along with additional protection such as **Sender Spoof Protection**.

Enable or disable the SPF features from the **Inbound Settings > Sender Authentication** page. To configure, see How to Configure Sender Policy Framework.

Sender Policy Framework (SPF)

SPF allows domain owners to publish authorized mail servers in DNS using **TXT records**. When Email Gateway Defense receives an email, it checks the **envelope-from** domain against the sending IP and the domain's SPF record.

SPF Result Types

- **Pass** – The sending IP is authorized by the domain's SPF record.
- **Fail (Hard Fail)** – The SPF record explicitly states that the IP is not authorized (e.g., -all).
- **Soft Fail** – The SPF record suggests that the IP is not authorized but does not require rejection (e.g., ~all).
- **Neutral** – No definitive authorization or rejection (e.g., ?all).
- **None** – No SPF record found for the domain.

Configuration Options

- **Action on SPF Hard Fail**
  - **Off** – No action taken on hard fail.
  - **Quarantine** – Messages with SPF hard fail are quarantined.
  - **Block** – Messages with SPF hard fail are blocked. This is the default setting.
- **Action on SPF Soft Fail**
  - **Off** – No action taken on soft fail. This is the default setting.
  - **Quarantine** – Messages with SPF soft fail are quarantined.
  - **Block** – Messages with SPF soft fail are blocked.
- **Block on No SPF Records**
  - **Off** – No action taken if the domain lacks an SPF record. This is the default setting.
  - **Quarantine** – Messages from domains without SPF records are quarantined.
  - **Block** – Messages from domains without SPF records are blocked.
- **SPF Exemptions**
  - You can exempt specific domains from SPF checks.

Exemptions reduce protection and increase the risk of spoofing.

DomainKeys Identified Mail (DKIM)

DKIM uses cryptographic signatures to verify that the message content has not been altered and that it was sent by a domain authorized to sign messages.

Key Details

- DKIM validates the domain in the d= tag of the DKIM signature, not the header From domain.
- Domain-based Message Authentication, Reporting & Conformance (DMARC) checks alignment between the header From domain and the DKIM d= domain.
- Adding or modifying content after signing, such as appending disclaimers, will break DKIM. Configure disclaimers before DKIM signing or disable signing for those messages.

Configuration Options

- **Block** – Emails that fail DKIM validation are blocked.
- **Quarantine** – Emails that fail DKIM validation are quarantined.
- **Off** – DKIM signatures are not evaluated. This is the default setting.
  Note: This applies to independent DKIM checks and does not impact DMARC evaluation and enforcement.
- **DKIM Exemptions** – Allows specific domains to bypass DKIM checks. Use the domain found in the DKIM signature d=.

Exemptions weaken authentication and should be limited in use.

Domain-based Message Authentication, Reporting & Conformance (DMARC)

DMARC builds upon SPF and DKIM to protect the **header From** domain, specifies how receivers should handle messages that fail authentication, and provides reporting.

Key Details

- **DMARC evaluation takes precedence over all independent sender authentication checks** (SPF, DKIM, and related policies).
- If a domain's DMARC policy is in enforcement mode (reject or quarantine), that policy determines the final action, regardless of SPF or DKIM results or exemptions.

- DMARC exemptions are based **only on the header From domain**, ensuring RFC compliance.
- Avoid excessive exemptions; these weaken protection and increase the risk of spoofing.

Configuration Options

- **Yes** – Applies DMARC policy checks to inbound mail.
- **No** – DMARC checks are not performed on inbound mail.
- **DMARC Exemptions** – Allows specific domains to bypass DMARC checks. You will enter the Header From domain.

Exemptions should be limited to trusted domains.

Sender Spoof Protection

Enable Sender Spoof Protection on Email Gateway Defense **Domain Settings** page when your domain does NOT have any DNS sender authentication settings, such as SPF or DMARC. 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**.

Select **Yes** to use Sender Spoof Protection to block emails from senders using your domain name. This means that Sender Spoof Protection will block emails if the domain used in either the **Header From** or **Envelope From** fields matches your domain in the **Envelope To** field.

Important Notes

- This feature does **not** protect against cross-domain spoofing within an account.
- When Sender Spoof Protection is enabled, SPF, DKIM, and DMARC checks are **not performed** on these messages because they are blocked based on the From/To domain match.

Bypass Sender Spoof Protection

Create a sender policy and select **Exempt** as the sender policy on the **Inbound Settings** > **Sender Policies** page.

Reverse DNS Check (No PTR)

Email Gateway Defense can block messages from IP addresses that do not have a valid PTR (reverse DNS) record. PTR records map an IP address to a hostname and are commonly required for legitimate mail servers.

Configuration Options

- **Enable No PTR Check**
  - **Yes** – Block messages from IP addresses without a valid PTR record**.** This is the default setting.
  - **No** – Do not block messages based on PTR records.

Important Notes

- This check is independent of SPF, DKIM, and DMARC.
- While useful for blocking poorly configured or suspicious servers, enabling this option may block legitimate mail from servers without PTR records.

Best Practices

- Publish SPF, DKIM, and DMARC for your domain.
- Avoid exemptions unless absolutely necessary.
- Monitor DMARC reports to identify unauthorized senders.
- Use all three mechanisms (SPF, DKIM, DMARC) together for maximum protection.