Sender Authentication

https://campus.barracuda.com/doc/96022989/

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

Sender Authentication mechanisms enable Email Gateway Defense to protect your network and users from spammers who might "spoof" a domain or otherwise hide the identity of the true sender.

Sender Policy Framework

If you have Sender Policy Framework (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 Email Gateway Defense IP ranges to your SPF exemptions based on your Barracuda Networks instance. See Email Gateway Defense IP Ranges for a list of IP addresses based on your Barracuda Networks 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 an Email Gateway Defense 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. This setting applies only to inbound mail.

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, Email Gateway Defense makes the IP address of your sending mail server visible to the agent performing SPF verification on the recipient's end.

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

SPF Policy Settings

Messages that fail SPF check can be blocked or quarantined and are logged as such.

Specify **SPF checking** settings on the **Inbound Settings > Sender Authentication** page:

- **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.

Additionally, you can select to exempt specific IP ranges or domains from SPF verification.

Block on No SPF Records

Configuration options available when senders send mail from or through mail servers whose domains lack reverse MX records, or have no SPF records.

Specify **Block on No SPF Records** settings on the **Inbound Settings > Sender Authentication** page:

- **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.

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.

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.

Specify **Block on No PTR Records** settings on the **Inbound Settings > Sender Authentication** page:

- **Yes** – If a sending domain does not have a PTR record, the mail server is blocked and the mail is not delivered to the user.
- **No** – There is no query for any senders.

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 Email Gateway Defense is to exempt the IP addresses of trusted email servers from being scanned on the **Inbound Settings > IP Address Policies** page, then block their domain names on the **Inbound Settings > Sender Policies** page to prevent domain name spoofing.

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. This feature does not protect against cross-domain spoofing within an account.

Note that Sender Spoof Protection is for inbound mail only, and does not stop your domain from being spoofed at other mail servers.

Barracuda Networks strongly recommends setting up proper SPF, DKIM, and DMARC records to authenticate your emails. Once configured, disable Sender Spoof Protection to allow the service to leverage the newly created records to authenticate emails that use your domain and originate from outside the organization.

To bypass Sender Spoof Protection, create a sender policy and select **Exempt** as the sender policy on the **Inbound Settings > Sender Policies** page.

See Understanding the Domains Page for more information.

Domain-Based Message Authentication, Reporting, and Conformance

Domain-based Message Authentication, Reporting, and Conformance (DMARC) is a sender email authentication mechanism that provides protection against phishing attacks, and improves spam accuracy by blocking spam in spoofed messages. DMARC is built on top of the email authentication mechanisms Sender Policy Framework (SPF) and DomainKeys Inspection (DKIM); you must have both an SPF and a DKIM record published for the domain to set DMARC policies.

Important

DMARC overrides DKIM and SPF settings if the following conditions are true:

- DMARC is enabled
- The sender's domain is not exempted from DMARC
- The sender's domain has a valid DMARC DNS TXT record (_dmarc.*example.com*)
- The policy specified by the sender's DMARC record indicates **block** or **quarantine**

The Link Protection feature in Email Gateway Defense will change the body hash of the email as the body is changed. If you are using DMARC inspection on the mail server side, disable Link Protection in Email Gateway Defense.

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

Specify DMARC policy settings on the **Inbound Settings > Sender Authentication** page:

- **Yes** – DMARC enables a sending domain to specify policy for messages that fail DKIM or SPF. This is the default setting.
- **No** – Email Gateway Defense does not run DMARC checks for inbound messages and the SPF and DKIM policy settings are used to verify the IP address range and sending domain.

Additionally, you can select to exempt specific domains from DMARC verification.

DomainKeys Inspection

> Appending a footer to outbound messages will cause outbound messages to fail a DKIM check, affecting mail delivery for recipients who check for DKIM.

The DKIM email authentication method allows a sending domain to cryptographically sign outgoing messages. When a message is received from a domain, Email Gateway Defense verifies that the message is from the sending domain and that the message has not been tampered with.

DKIM uses a public and private key-pair system. An encrypted public key is published to the sending server's DNS records, and each outgoing message is then signed by the server using the corresponding private key. For incoming messages, when Email Gateway Defense sees that message is signed, it retrieves the public key from the sending server's DNS records and uses that key to validate the message's DKIM signature.

Specify DKIM policy settings on the **Inbound Settings > Sender Authentication** page:

- **Block** – Messages from a domain that fails DKIM verification are blocked. This is the default setting.
- **Quarantine** – Messages from a domain that fails DKIM verification are quarantined.
- **Off** – When set to Off, Email Gateway Defense does not run DKIM checks for inbound messages.

Additionally, you can select to exempt specific domains from DKIM verification.