Sender Authentication

https://campus.barracuda.com/doc/3866643/

This is a key feature of the Barracuda Email Security Gateway for protecting your network and users from spammers who might spoof a domain or otherwise hide the identity of the true sender. The following techniques are used to verify the "from" address of a message.

Mail Protocol (SMTP) Checking

The Barracuda Email Security Gateway can perform thorough checks on incoming email for RFC 821 compliance, require mail clients to introduce themselves with an SMTP "HELO" or "EHLO" command before stating a sender, and otherwise manage SMTP protocol to block spammers. See the **ADVANCED > Email Protocol** page for these and other optional SMTP settings.

Sender Spoof Protection

The Barracuda Email Security Gateway has the option to prevent spoofing of an organization's own domain by blocking emails with that domain name in the "From" field that are sent from outside the organization. Note that sender spoof protection should not be enabled if the organization sends messages from outside their internal email infrastructure (e.g., in the case of marketing bulk-mail services).

The **Sender Spoof Protection** feature can be configured at the global level from the **ADVANCED > Email Protocol** page or at the per-domain level on the **DOMAINS > Manage Domain > ADVANCED > Email Protocol** page. At the domain level, however, this feature is labeled as **Reject messages from my domain**.

Note that if the administrator enables **Sender Spoof Protection** at the global level, it will supersede any Allow List entry created at the per-user level by a *User*, *Helpdesk* or *Domain Admin* account holder.

Invalid Bounce Suppression

The **Invalid Bounce Suppression** feature is used to determine whether or not the bounce address specified in a message is valid. It is designed to reduce the number of bounce messages to forged return addresses; i.e., you don't want to get bounced messages from spammers who spoof your domain or email address. Every email sent from the Barracuda Email Security Gateway is tagged with

an encrypted password and expiration time. With **Invalid Bounce Suppression** enabled, any bounced email received by the Barracuda Email Security Gateway that does not include that tag is blocked. Each blocked message is recorded in the Message Log with the reason "Invalid Bounce".

To use the Invalid Bounce Suppression feature, you must configure Outbound Relay on the **BASIC > Outbound** page of the Barracuda Email Security Gateway. For more details about Outbound Relay, refer to How to Route Outbound Mail From the Barracuda Email Security Gateway.

Configure Invalid Bounce Suppression on the **BLOCK/ACCEPT > Sender Authentication** page and enter a **Bounce Suppression Shared Secret** as a non-null password which will be included in the headers of valid emails sent from and bounced back to the Barracuda Email Security Gateway. Email bounces that don't include the password will be blocked if this feature is enabled. In a clustered environment, the **Bounce Suppression Shared Secret** will be synchronized across all Barracuda Email Security Gateways in the cluster.

Sender Policy Framework (SPF)

If you are using the Barracuda Cloud Protection Layer (CPL) in front of your Barracuda Email Security Gateway, SPF settings do not apply. This is because the CPL IP addresses are designated known forwarders, so they are exempt from SPF failures on the Barracuda Email Security Gateway.

Sender Policy Framework (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 the delivery of messages. SPF works by having domains publish reverse MX records to display which machines (IP addresses) are designated as valid mail sending machines for that domain. When receiving a message from a domain, the recipient can check those records to make sure mail is coming from a designated sending machine. If the message fails the SFP check, it may be spam. Enabling this feature does create more performance overhead for the system due to the multiple DNS queries needed to retrieve a domain's SPF record; for this reason, the default setting for the **Enable SPF** feature on the **BLOCK/ACCEPT > Sender Authentication** page is *No* (off).

Messages that fail SPF check can be tagged or blocked and will be logged as such. Messages that pass SPF checks will still be scanned for spam. The recommended setting is to tag messages identified by SPF as spam, so that if there is any possibility that a message is legitimate, it will be allowed to go on to the next stage of processing.

Exemptions from SPF Checking - Known Forwarders

You may specify a list of Known Forwarder IP addresses, on the **BASIC > IP Configuration** page, which will be ignored when performing SPF checks, as well as rate control and IP Reputation checks. Known Forwarders are mail servers that are set up specifically to forward email to the Barracuda Email Security Gateway from outside sources. The Barracuda Email Security Gateway scans the IP addresses in the **Received From** headers list of each email and performs an SPF check on the first IP address that is not in the list of Known Forwarders.

DomainKeys Identified Mail (DKIM) Inspection

DomainKeys is a method of email authentication that enables a sending domain to cryptographically sign outgoing messages, allowing the sending domain to assert responsibility for a message. When receiving a message from a domain, the Barracuda Email Security Gateway can check the signature of the message to verify that the message is, indeed, from the sending domain and that the message has not been tampered with. Because most spam messages contain spoofed addresses, DomainKeys can help greatly in the reduction of spam.

DomainKeys uses a public and private key-pairs system. An encrypted public key is published to the sending server's DNS records and then each outgoing message is signed by the server using the corresponding encrypted private key. For incoming messages, when the Barracuda Email Security Gateway sees that a message has been signed, it will retrieve the public key from the sending server's DNS records and then compare that key with the message's DomainKeys signature to determine its validity. If the incoming message cannot be verified, the Barracuda Email Security Gateway knows it contains a spoofed address or has been tampered with or changed.

The benefits of enabling this feature include:

- Email sender is validated
- Email body is validated
- Validation through DNS is difficult to foil
- DomainKeys works well with email forwarding because it doesn’t deal with the relay server IP address

You can choose to tag, block or quarantine both DKIM signed messages that fail the DKIM database check as well as unsigned messages, depending on how you configure **DomainKeys Inspection** on the **BLOCK/ACCEPT > Sender Authentication** page. You can also exempt domains from being tagged, quarantined or blocked if they fail this check. As stated elsewhere in this guide, it is safest to NOT exempt domain names from any kind of spam filtering due to the possibility of domain name spoofing by spammers.

DomainKeys inspection does require more CPU resources to encrypt & decrypt the key and is turned off by default. Messages that pass DKIM checks will still be scanned for spam.

Important: DKIM is used to prevent man-in-the-middle attacks. Therefore, if an email is amended, appended or truncated in any way between signing the message and checking the signature, it will fail the check on the receiving server. This means that Barracuda Email Security Gateway *should not be configured to encrypt or add footer information to outgoing emails when DKIM has been applied.* It also means that the user's mail client should be correctly configured in compliance with best standards, to ensure that the character limits for each line in an outgoing HTML email do not exceed 990 characters. Otherwise, the Barracuda email agent will insert a line break to ensure compliance. This could cause DKIM failure, because when the receiving server checks the signature, the contents of the received email will vary from the email that was sent.

Domain-Based Message Authentication, Reporting, and Conformance (DMARC)

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). To set DMARC policies, you must have both an SPF and a DKIM record published for the domain. This feature is available using the Cloud Protection Layer (CPL). For more information about DMARC, see DMARC Verification.

Custom policies

Organizations can define their own allowed sender domains or email addresses for sender authentication using the **BLOCK/ACCEPT > Sender Filters** page, but the safest way to indicate valid senders on the Barracuda Email Security Gateway is to add the IP addresses of trusted email servers to the Allow List on the **BLOCK/ACCEPT > IP Filters** page, then add their domain names to the Block List (block, quarantine, or tag) on the **BLOCK/ACCEPT > Sender Filters** page to prevent domain name spoofing.

On the **BLOCK/ACCEPT > Sender Filters** page, sender filters check the **Envelope From**, **Header From** and **Reply To** fields.