Sender and Recipient Analysis

https://campus.barracuda.com/doc/96023020/

Sender Analysis

Use the **Inbound Settings > Sender Policies** page to exempt, quarantine, or block messages based on username, domain, or email address. Email Gateway Defense applies header scanning to both the Header and the Envelope From fields. In the Header field, only the email address portion is checked. Note that wildcards, for example, asterisk (*) or the @ sign are not supported. For example: *@`customer.com` is recognized as `customer.com`

Sender policies allow you to exempt, quarantine, or block messages as follows:

- **User** – Only the *username* part of the sender's email address is checked. For example, adding a policy for a username of *info* means that the policy you select is applied to all inbound messages from senders with an email address of info@*sendingdomain.com* where *sendingdomain.com* represents any sending domain.
- **Domain** – Only the domain part of the email address is checked.
- **Email address** – The entire email address is checked.

Policies

- **Quarantine** – Messages from the entered sender are always quarantined.
- **Block** – Blocking a domain automatically blocks all subdomains. Note that blocking email addresses is not recommended as spammers rarely, if ever, use the same sender email address more than once.
- **Exempt** – When you add a domain, subdomain, or email sender and select **Exempt**, Email Gateway Defense always accepts, or allows those messages. Messages from allowed senders bypass spam scoring, Intent Analysis, and content filters, however, virus scanning and rate control are still applied. To bypass Sender Policy Framework (SPF) checking, add the **Envelope From** IP to exempt the sender. Barracuda Networks also recommends adding the sender IP or domain to the **SPF Exemptions** list on the **Inbound Settings > Sender Authentication** page.

  Warning: Spammers can use an exempt email address to bypass filtering; as such, allowing trusted IP addresses is a more reliable way to identify trusted domains. Add trusted IP addresses to your allow list on the **Inbound Settings > IP Address Policies** page. If the email sender and recipient addresses are the same, Email Gateway Defense disregards the exempt email address and processes the mail normally. This is done because spammers know that users tend to allow their own email address.

Recipient Analysis

Use the **Inbound Settings > Recipient Policies** page to specify whether to always **Scan** or always **Exempt** (allowed) a recipient email address. Exempt (allowed) recipients bypass spam scoring (see **Enable Cloudscan** on the **Inbound Settings > Anti-Spam/Anti-Virus** page) as well as all other block lists. Virus scanning still applies.