IP Analysis - Inbound

https://campus.barracuda.com/doc/16920/

Important
When entering an IP range in Email Gateway Defense, it is *critical* that the starting IP address is valid. For example, the following table shows an invalid and the corrected IP range:

Invalid (IP – Netmask)	Correct (IP – Netmask)
• 209.222.86.3-255.255.255.0 (256 address range) • 209.222.84.0-255.255.248.0 (2048 address range)	• 209.222.82.0-255.255.255.0 • 209.222.82.0-255.255.248.0

Additional Resource

To find the correct starting and ending IP addresses in a range,

1. Go to the MXToolbox Subnet Calculator.
2. Enter an IP address in your range and the netmask, and click **View Subnet** to view your starting IP address.

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

Create Custom IP Policies

Once the true sender of an email message is identified, the reputation and intent of that sender should be determined before accepting the message as valid, or "not spam". The best way to address both issues is to know the IP addresses of trusted email senders and forwarders and define those as exempt from scanning by adding them to a list of known good senders.

When checking policies, the policies are processed from smallest network bit to largest. This means that when multiple policies result in exemptions or blocks nested within larger ranges of exemptions or blocks, only the policy with the smallest networks bits (largest range) would be applied, regardless of nested values. For example, a block policy that starts within a range of 1.2.3.0 and netmask of 255.255.255.0, then an exemption of IP 1.2.3.4 and netmask of 255.255.255.255 would still get blocked. The converse would also be true; the policy covering the largest range is applied, nested policy IPs and ranges are not extracted.

Add exempt/trusted sender IP addresses and block those you know are not trusted on the **Inbound**

Settings > IP Address Policies page.

> Barracuda Networks does not recommend exempting domains because spammers may spoof domain names. When possible, it is recommended that you exempt by IP address only.

You can create a list of **Trusted Forwarders** by specifying one or more IP addresses of machines that you have set up to forward email to Email Gateway Defense from outside sources. Email Gateway Defense exempts any IP address in this list from Rate Control, Sender Policy Framework (SPF) checks, and IP Reputation. In the Received headers, Email Gateway Defense continues looking beyond a Trusted Forwarder IP address until it encounters the first non-trusted IP address. At this point, Rate Control, SPF checks, and IP Reputation checks are applied. Configure on the **Inbound Settings > IP Address Policies** page.