**Requirement 1**: IP Whitelisting (Allow only specific networks)

**Requirement 2**: API Rate Limiting (Allow only 1000 requests per minute)

We are using **Cloud Armor** to fulfil the above two requirements. We created a **single Cloud Armor policy** that includes rules for both **IP whitelisting** and **API rate limiting**.  
  
Example Rule:  
request.path.matches('/qorecommunicationreceiver/webhook/secure\_conversation\_message\_reply') && (inIpRange(origin.ip, '198.167.186.192/26') || inIpRange(origin.ip, '167.103.120.0/23') || inIpRange(origin.ip, '165.225.120.0/23') || inIpRange(origin.ip, '136.226.232.0/23'))  
  
**request.path.matches(...)**: This checks if the request is targeting the path /qorecommunicationreceiver/webhook/secure\_conversation\_message\_reply.  
 **inIpRange(origin.ip, 'X.X.X.X/XX')**: This checks if the IP address of the incoming request (origin.ip) is within one of the allowed ranges (e.g., '198.167.186.192/26').

**OR (||)**: You’re using OR to allow multiple IP ranges, so if the request is from any of the listed ranges, it will be allowed.  
  
Only requests coming from the specified IP ranges (e.g., 198.167.186.192/26, 167.103.120.0/23, etc.) will be allowed to access the /qorecommunicationreceiver/webhook/secure\_conversation\_message\_reply path.

Any request coming from an IP outside of those ranges will be blocked.  
  
**Rate Limiting Setup**:

* + You can set a rule to allow **only 1000 requests per minute** from an IP address.
  + If an IP exceeds the 1000 requests within a minute, Cloud Armor will block or throttle further requests.

**Steps:**

* In the **Google Cloud Console**, under **Cloud Armor**, you create a **security policy** and define the **rate limit rule** (1000 requests per minute).
* Cloud Armor will automatically enforce this rule for all incoming traffic.