### **Part 1: Configure the Web Server to Listen on a New Port**

You need to tell your web server to accept incoming connections on an additional port besides the standard ones (80 and 443).

**For Apache:**

1. **Connect to your VM:** Use SSH to log in to your VM instance.
2. **Edit the ports configuration file:** Open the ports.conf file, which is typically located at /etc/apache2/ports.conf.  
     
   sudo nano /etc/apache2/ports.conf
3. **Add the new port:** At the end of the file, add a new Listen directive for your chosen port. For this example, let's use 8080

# The default configuration

Listen 80

<IfModule ssl\_module>

Listen 443

</IfModule>

# Add a new port for your admin site

Listen 8080

**Save the file** and exit the editor.

**Part 2: Host Your Admin Website on that Specific Port**

Now, you need to create a separate configuration for your admin site that tells the web server what content to serve when a request comes in on the new port.

**For Apache:**

1. **Create the directory for your admin site:**

sudo mkdir -p /var/www/admin

1. **Create a sample index file in the new directory to test**

**sudo sh -c 'echo "<h1>Admin Page</h1>" > /var/www/admin/index.html'**

1. **Create a new virtual host configuration file: A good location is /etc/apache2/sites-available/admin.conf.**

**sudo nano /etc/apache2/sites-available/admin.conf**

1. **Add the virtual host block: Add the following configuration, making sure the DocumentRoot points to your new directory.**

**<VirtualHost \*:8080>**

**ServerName youWebName.com**

**DocumentRoot /var/www/admin**

**# SSL/TLS Configuration**

**SSLEngine on**

**SSLCertificateFile /etc/letsencrypt/live/youWebName.com/fullchain.pem**

**SSLCertificateKeyFile /etc/letsencrypt/live/youWebName.com/privkey.pem**

**# Log files**

**ErrorLog ${APACHE\_LOG\_DIR}/admin\_error.log**

**CustomLog ${APACHE\_LOG\_DIR}/admin\_access.log combined**

**</VirtualHost>**

1. **Enable the new site and restart Apache:**

**sudo a2ensite admin.conf**

**sudo systemctl restart apache2**

**Part 3. Create Fire Wall Rules**

**Go to the Google Cloud Console: Open your web browser and navigate to the Google Cloud Console.**

**Navigate to Firewall Rules:**

* **In the navigation menu on the left, go to VPC network > Firewall.**
* **This will take you to a page that lists all your existing firewall rules.**

**Click "Create Firewall Rule": At the top of the page, click the Create firewall rule button.**

**Fill in the Rule Details: You'll be taken to a form to configure the new rule.**

* **Name: Give the rule a descriptive name. Something like allow-admin-port-8080 or admin-page-access is a good choice.**
* **Network: Select the VPC network that your VM instance is connected to. In most cases, this will be the default network unless you've created a custom one.**
* **Priority: You can leave this at the default value (e.g., 1000). Lower numbers are processed first, but for a new rule, the default is fine.**
* **Direction of traffic: Select Ingress. This means the rule applies to traffic coming *into* your VM.**
* **Action on match: Select Allow.**
* **Target: This specifies which VMs the rule applies to.**
  + **The simplest option is to select All instances in the network.**
  + **A more precise method is to use Specified target tags. If your VM has a network tag (e.g., http-server), you can enter that tag here. If not, the first option is fine.**

**Configure the Source Filter (CRITICAL SECURITY STEP):**

* **Source filter: Choose IPv4 ranges.**
* **Source IPv4 ranges: This is where you specify who is allowed to access the port.**
  + **For Secure Access: Enter the public IP address of your local PC and your colleagues' PCs. You can find your public IP by searching "what is my ip" on Google. Enter the IP addresses in CIDR notation, e.g., 203.0.113.1/32.**
  + **To add multiple IPs: You can add multiple IP addresses, each on a new line, like this:**

**Specify the Protocols and Ports:**

* **Protocols and ports: Select Specified protocols and ports.**
* **tcp: Check the box next to tcp and enter 8080 in the field provided.**

**Create the Rule:**

* **Review all the settings to ensure they are correct.**
* **Click the Create button at the bottom of the form.**