**Application Gate way**

An **Application Gateway** is a web traffic load balancer that operates at the **application layer (Layer 7)** of the OSI model. It's a crucial component for managing and securing web applications in cloud environments like Microsoft Azure.

**Key Functions:**

* **Load Balancing:** Distributes incoming web traffic across multiple backend servers (like virtual machines or containers) to ensure high availability, scalability, and optimal performance.
* **SSL/TLS Termination:** Decrypts incoming HTTPS traffic, offloading this processing from backend servers and improving their performance.
* **Web Application Firewall (WAF):** Provides protection against common web attacks like SQL injection, cross-site scripting (XSS), and DDoS attacks.
* **URL-Based Routing:** Routes traffic to specific backend servers based on the URL path in the incoming request.
* **Cookie-Based Session Affinity:** Ensures that requests from the same client session are always directed to the same backend server.
* **Content Caching:** Caches static content (like images and CSS files) to improve website performance and reduce load on backend servers.

**Benefits of using Application Gateway:**

* **Improved Performance:** Offloads SSL processing, distributes traffic efficiently, and caches static content.
* **Enhanced Security:** Protects against web attacks with built-in WAF capabilities.
* **High Availability:** Ensures continuous service availability by distributing traffic across multiple servers.
* **Scalability:** Easily scales to handle increasing traffic demands.
* **Centralized Management:** Provides a single point of management for web traffic routing and security policies.

**Features:**

1. It works on URL/path based routing.
2. It works on layer-7 of OSI model (application layer).
3. It supports HTTP & HTTPS based applications.
4. It supports WAF (Web Application Firewall).
5. It supports multiple Backend pools.
6. It can supports regional only.
7. It can be built in a Separate or Dedicated Subnet.
8. Public or private IP is assigned to a APPGW.

**Note:** In DNS IP to domain name mapping is know as Host A record.

**APPGW Configuration:**

1. Frontend IP
2. Backend pool
3. Heath probes
4. Load Balancer rules
5. Backend Settings: Here we configure the Backend protocol’s (HTTP &HTTPS) and backend port.
6. Listeners: Listeners act as the entry points for incoming traffic. They are responsible for intercepting and processing incoming requests based on their protocol, port, hostname, and IP address. (if our app is runs on port 443 then this 443 is a listener).

**Why we use Application Gate Way?**

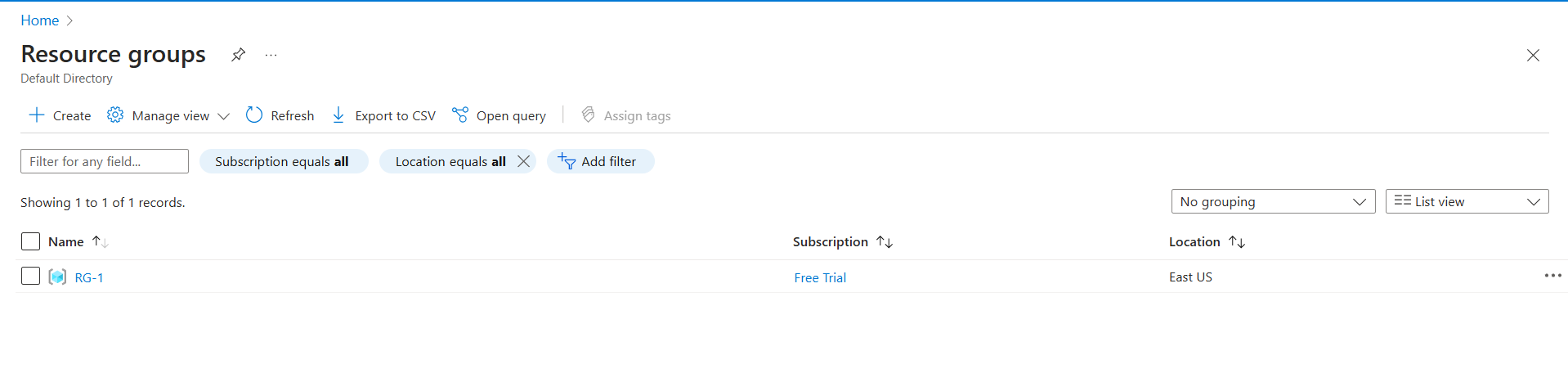
If our workloads are in different Server’s, to route the traffic among then based on URL or path we use the Application gate way.

**Note: Workloads on Different servers=>** having our Application in different servers like Home page of our application in one server, Business page in another server, and so on…

This pages are isolated or configured based on URL or Path like WWW.ICIC.com, WWW.ICIC/Business.com and so on.

Let’s create the Application gate way practically.

Step1: create the resource group (RG-1)



Step2: Create the Virtual Network (Vnet-1).

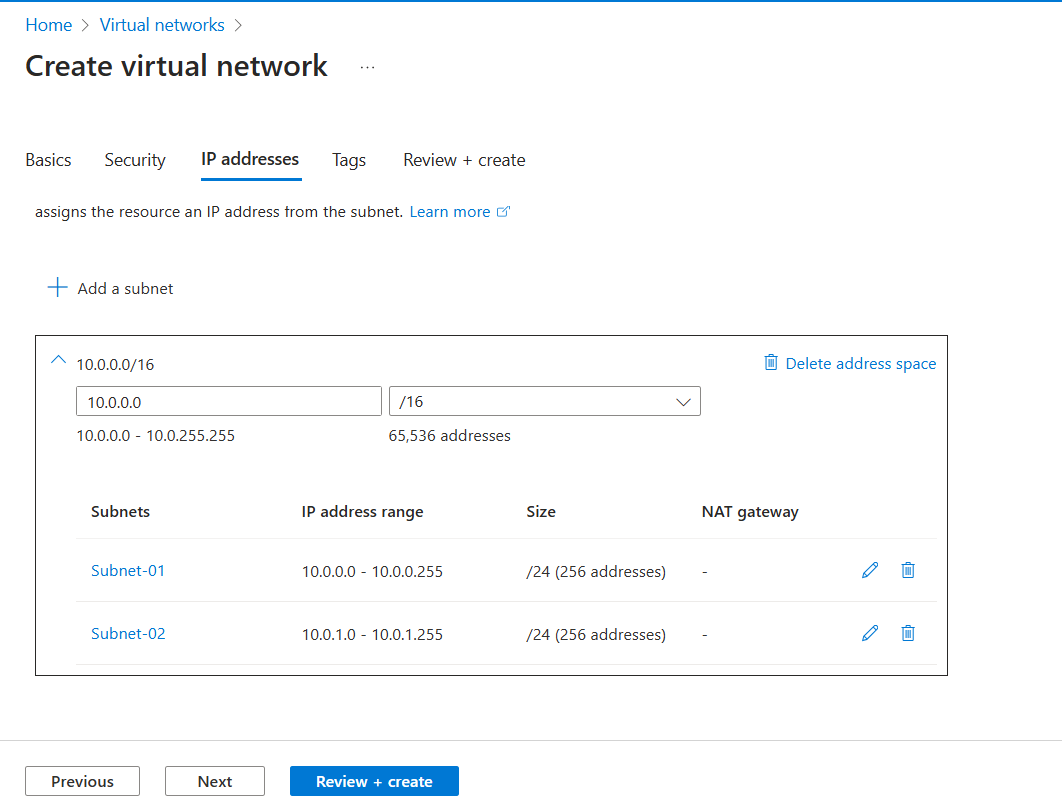


Fig: configuring of subnets.

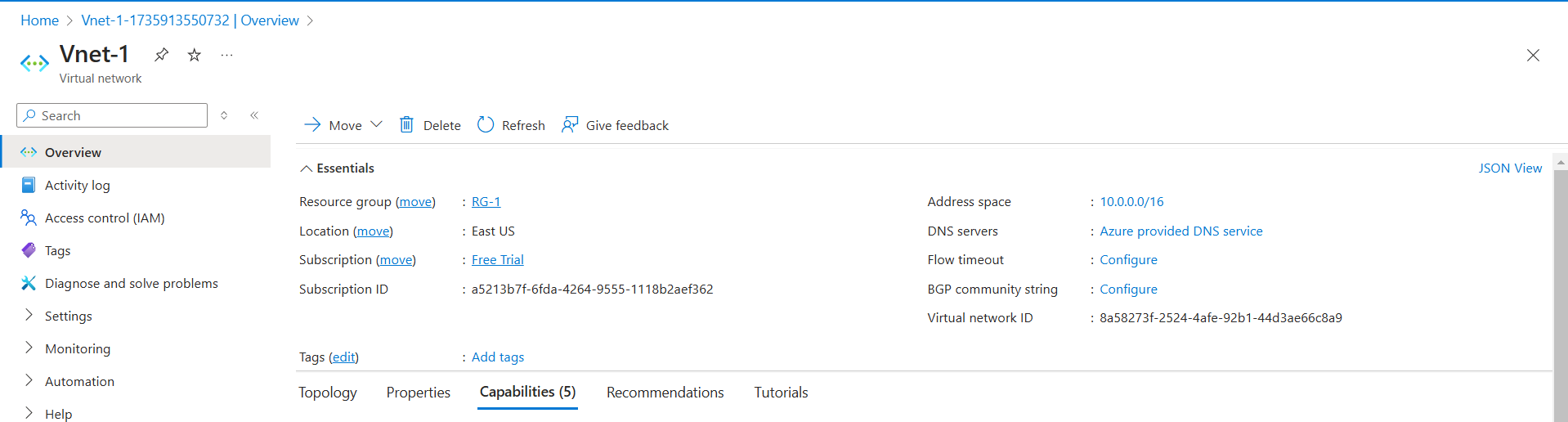


Fig: Virtual Network.

Step3: Creation of Virtual machines (VM-1 & VM-2) in same Virtual network (Vnet-1).

(Same region).

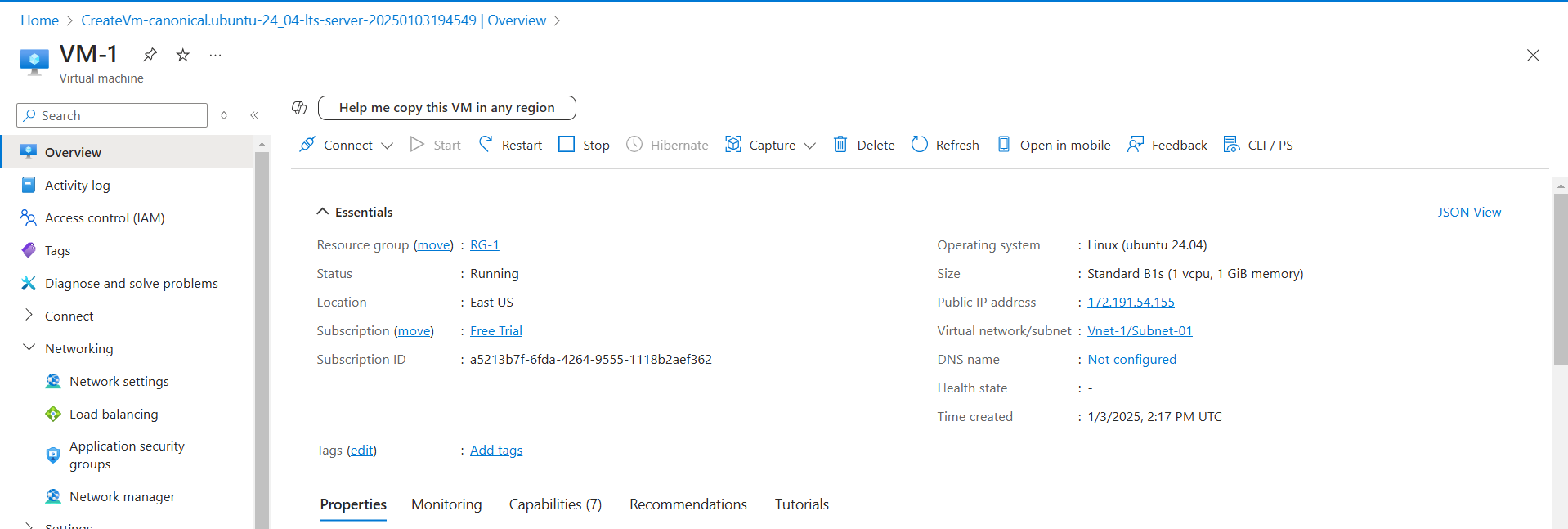
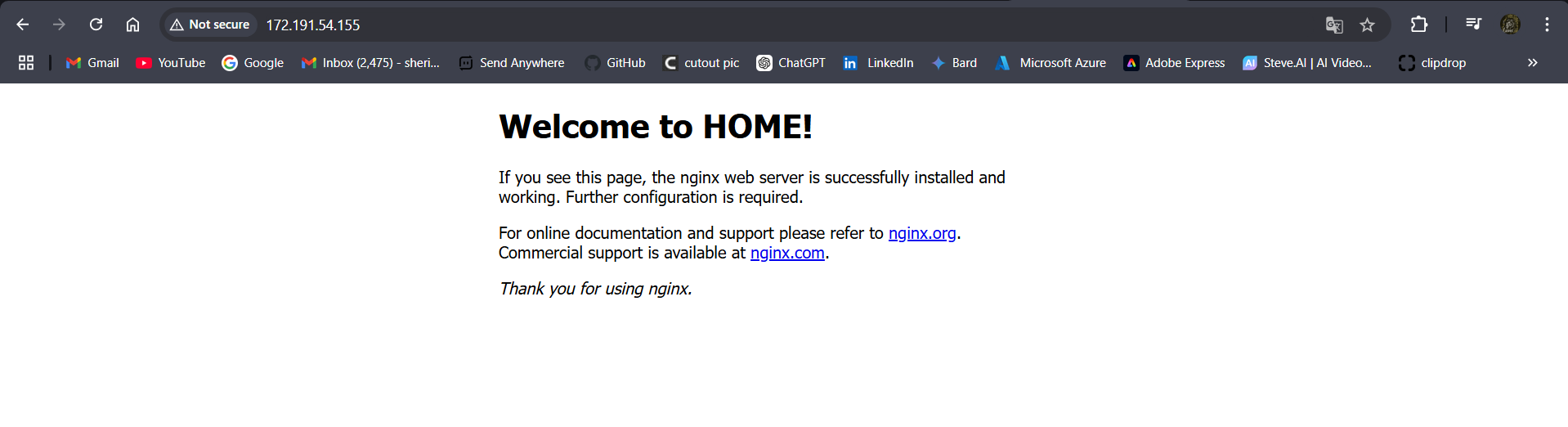


Fig: Virtual machine (VM-1) where Home page is deployed in it. (Path=”/”).



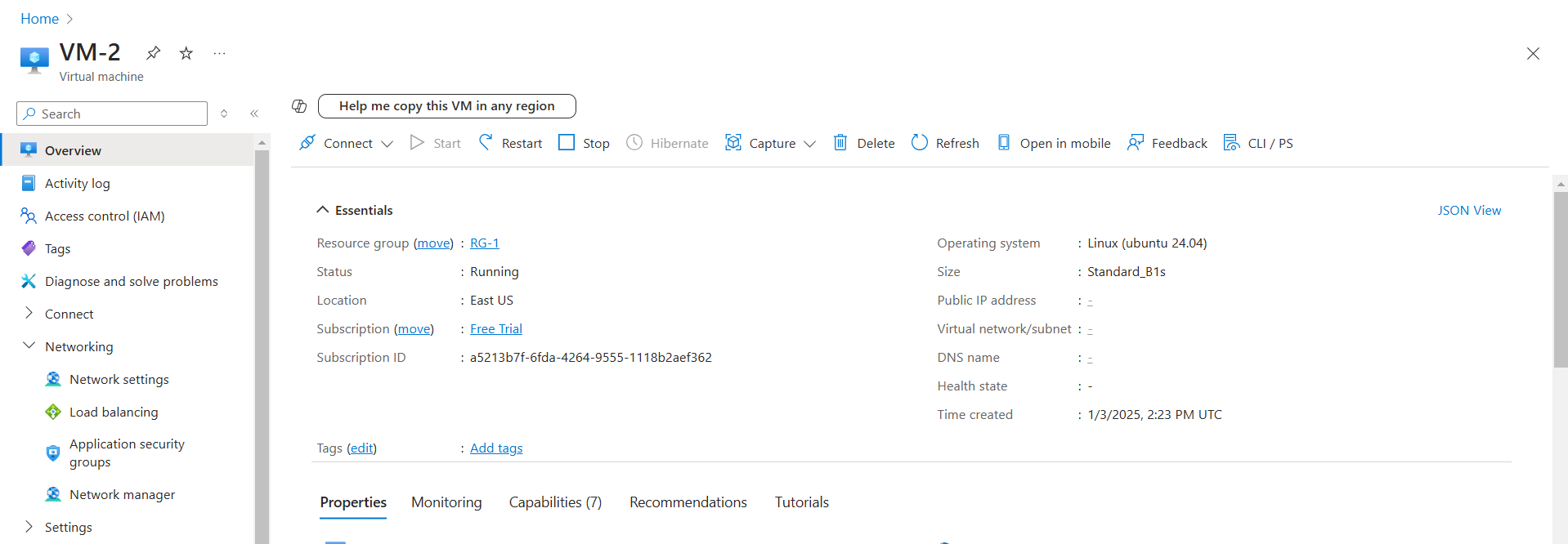
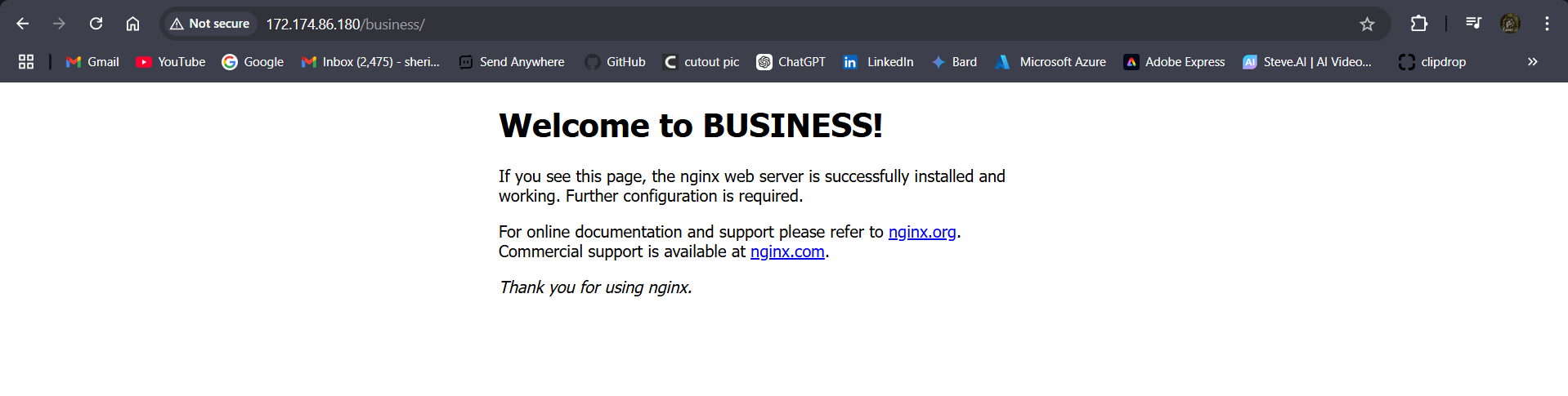


Fig: Virtual Machine (VM-2) in which Business page is deployed. (Path=”/business/”)



Step4: Create the Application Gate Way (APPGW).

**Note:** while creating APPGW it must and should require to create in dedicated Subnet.

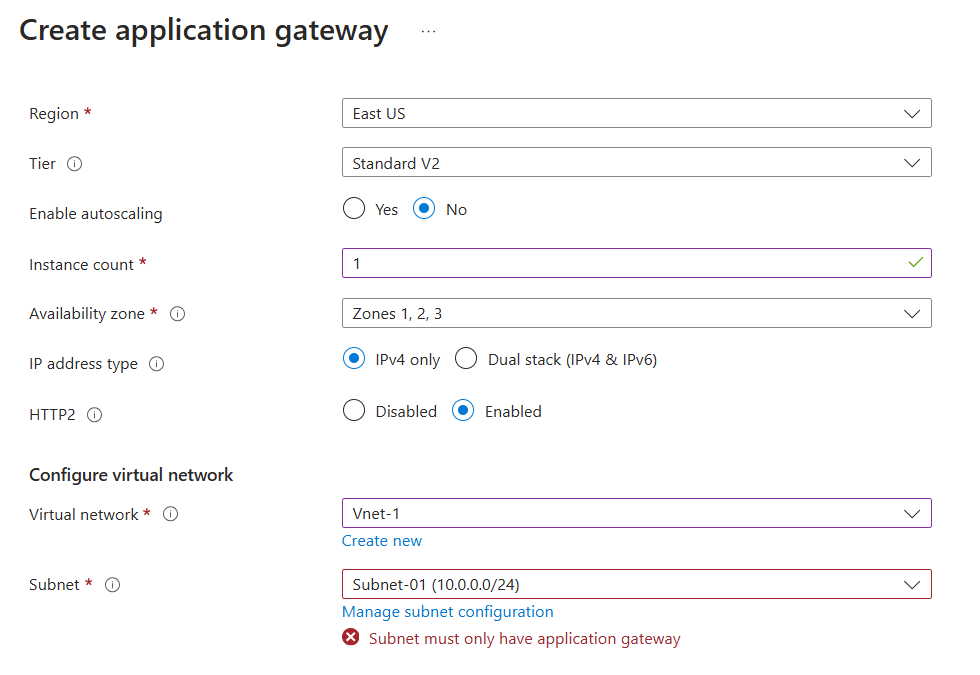


Fig: showing warning that while creating APPGW it must only have separate Subnet.

Note2: Ignore the Backend pool, routing rules and backed settings while creating the APPGW because it cannot show some of additional settings, in creating routing Rules like “Add multiple targets to create a path based rule”.

Case1: Creation of Backed pools.

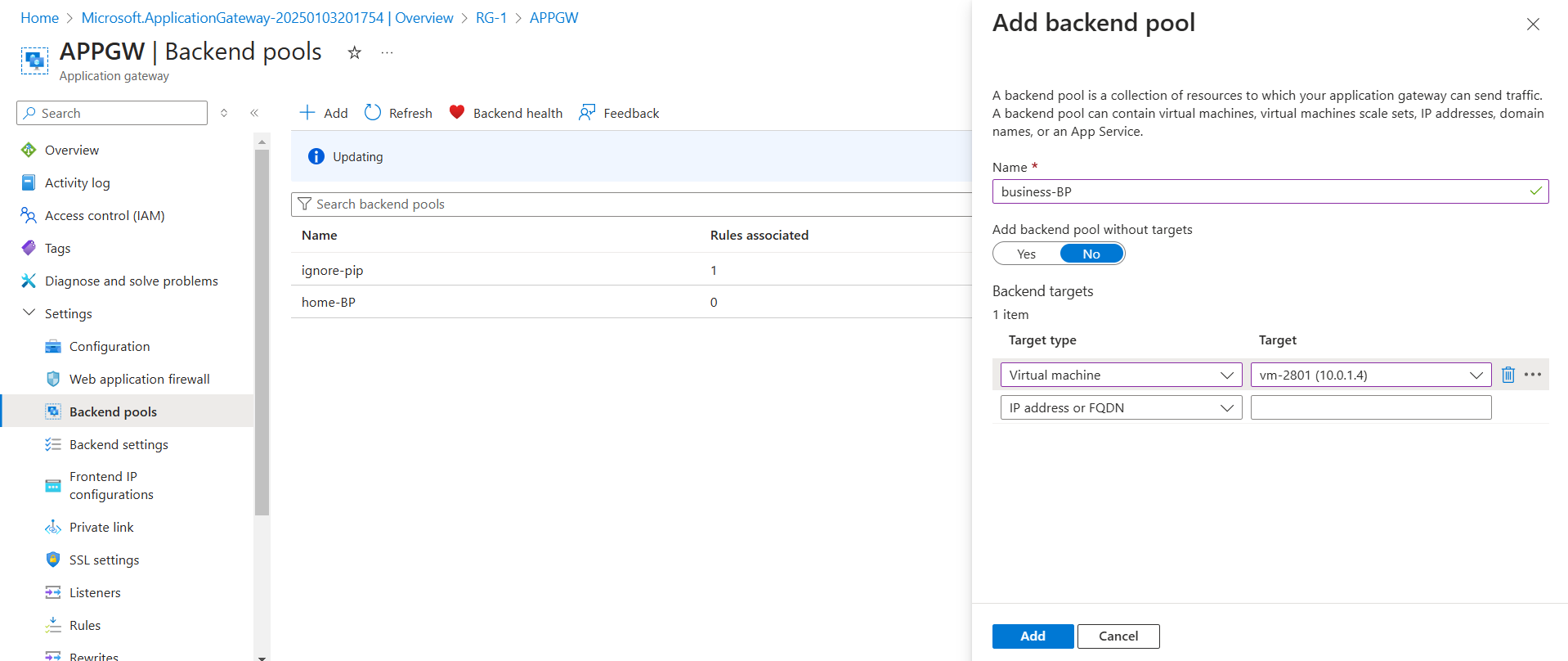
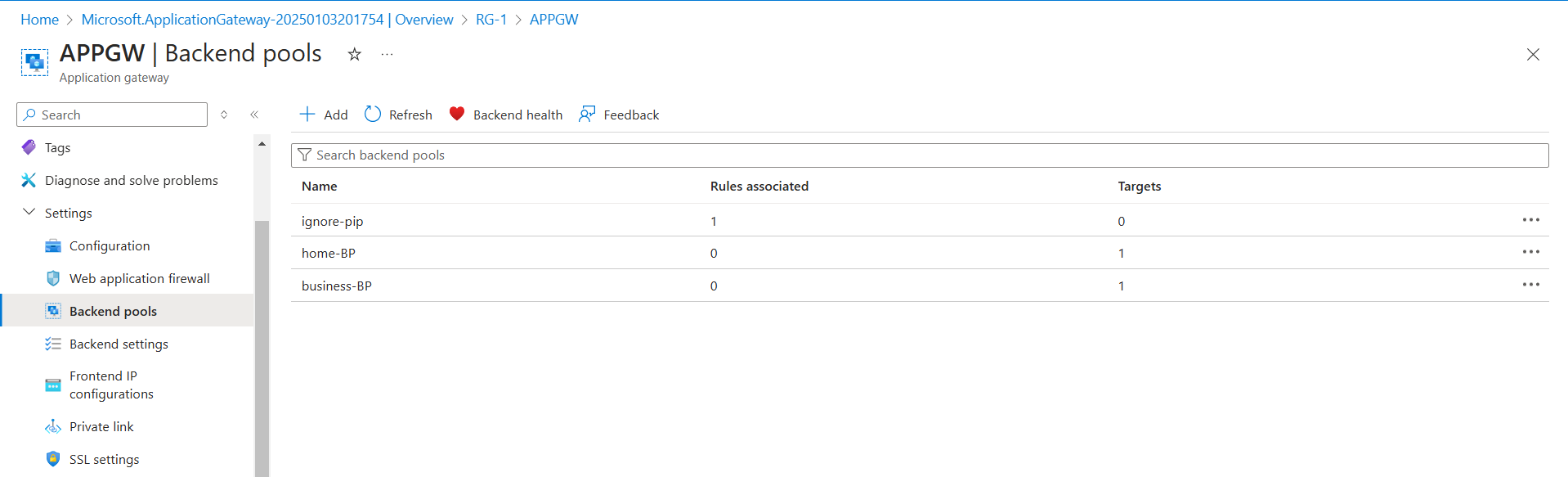


Fig: adding of Backend pools (home page & business page pool).



Case2: Adding of Backend Settings

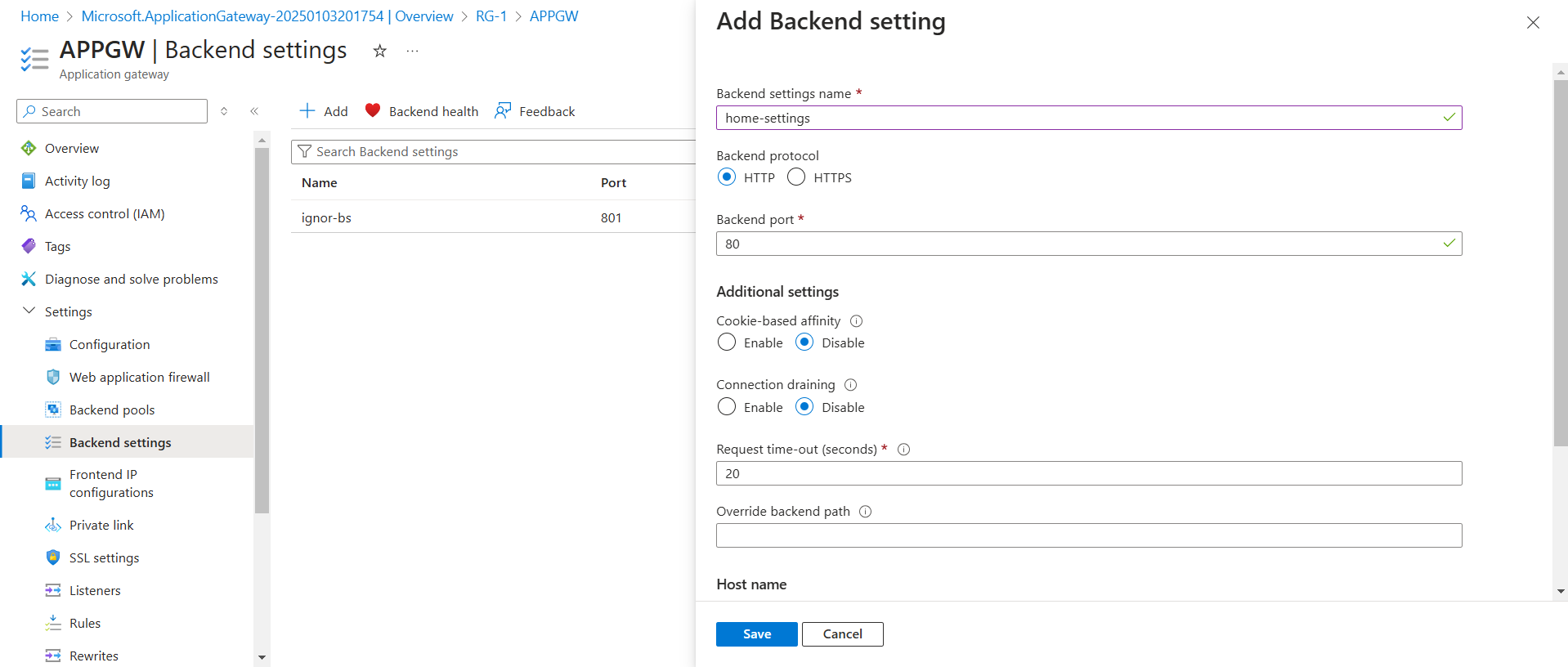
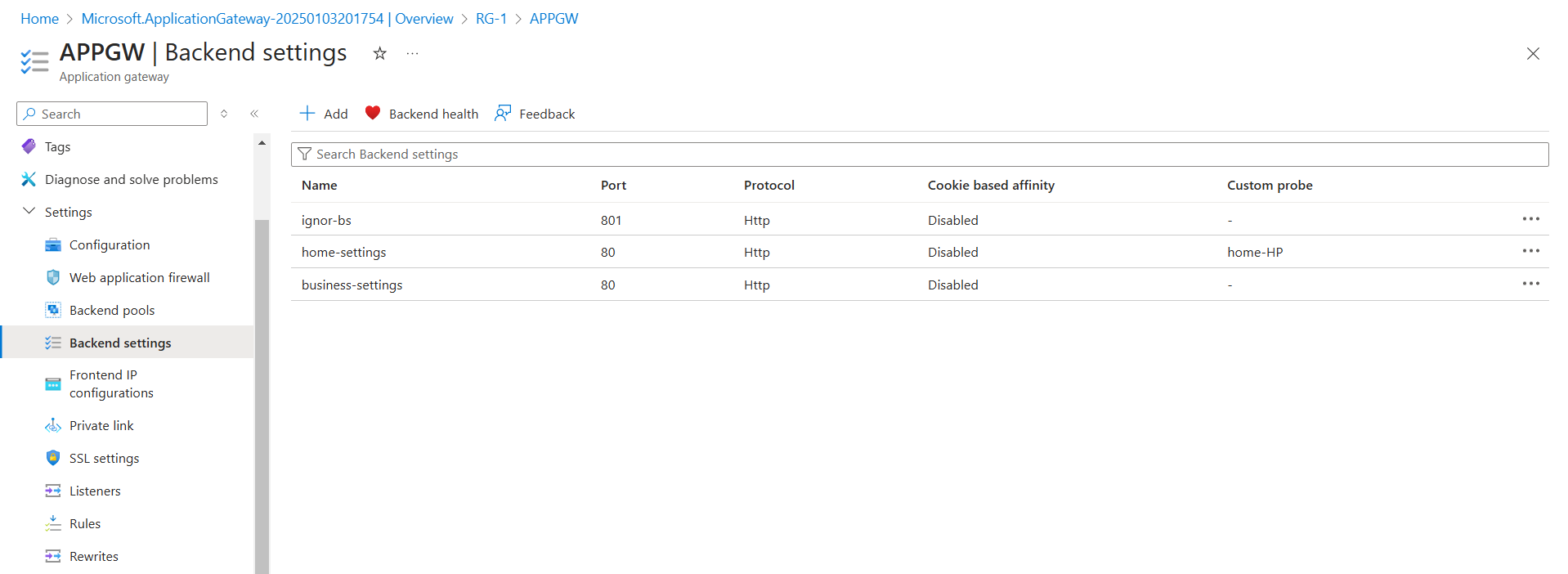
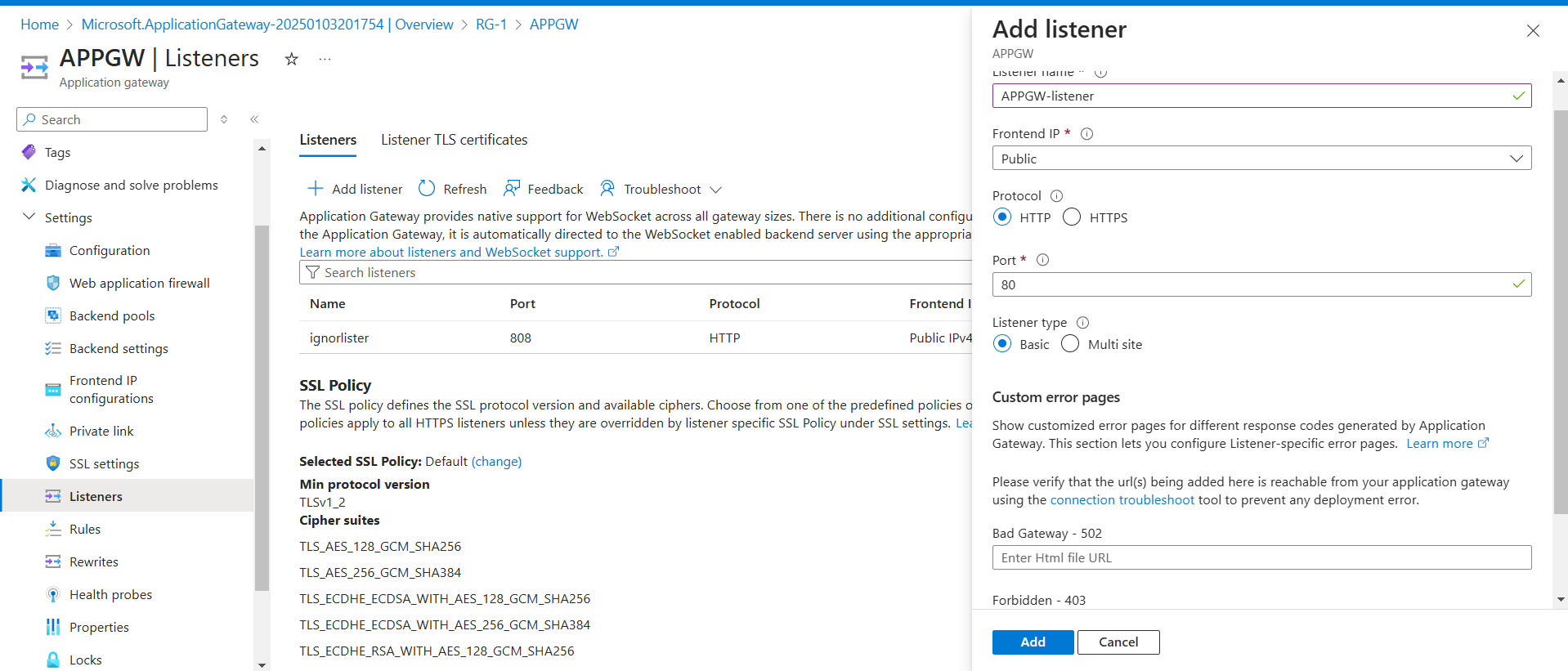


Fig: Adding of home & business page Backend settings



Case3: Adding of listeners.

Case4: Adding of Health probes

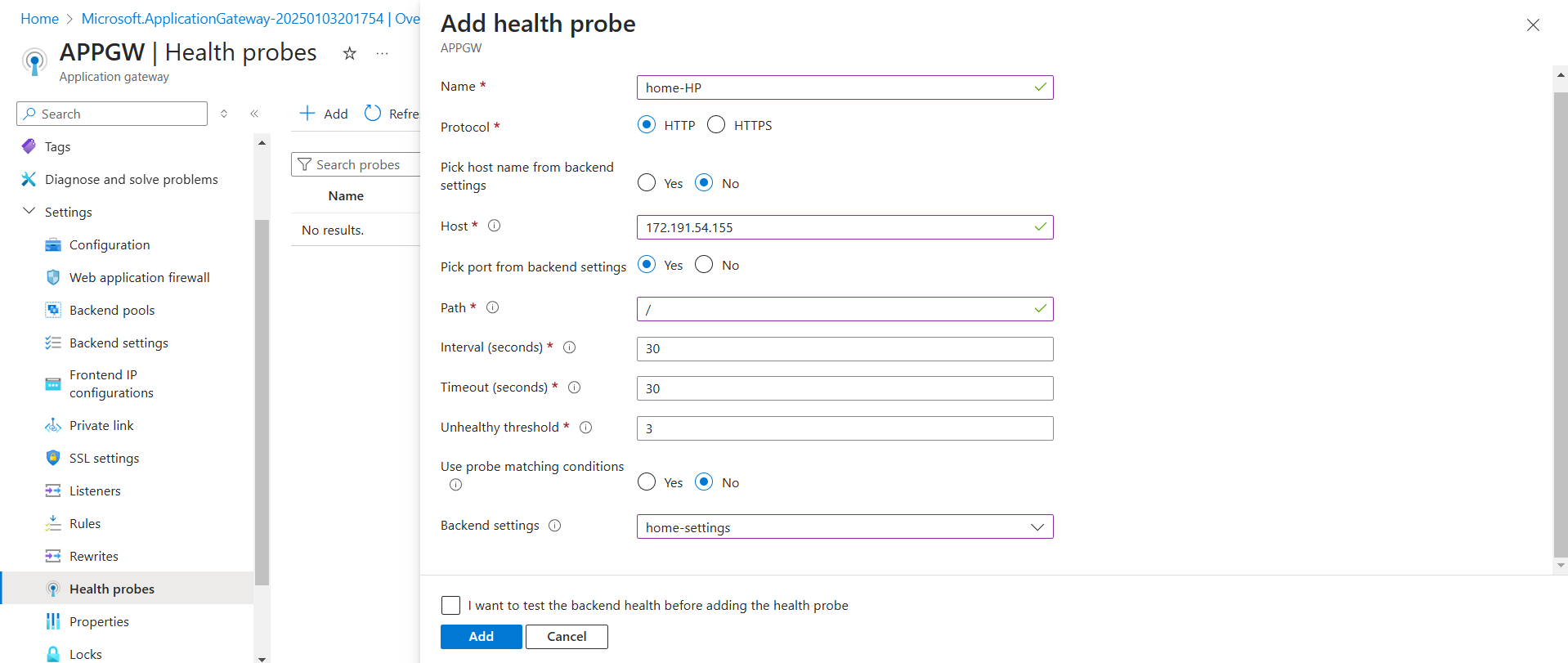


Fig: home page health probe.

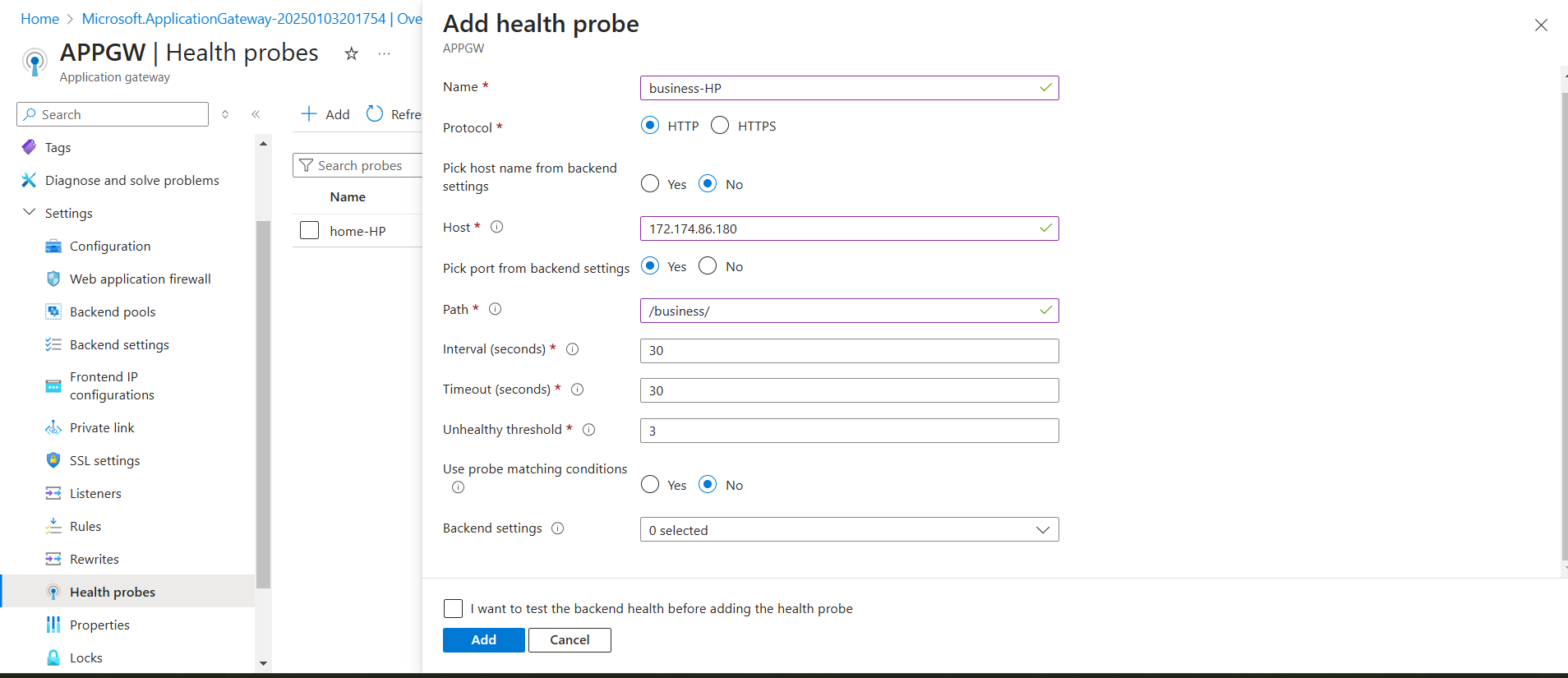
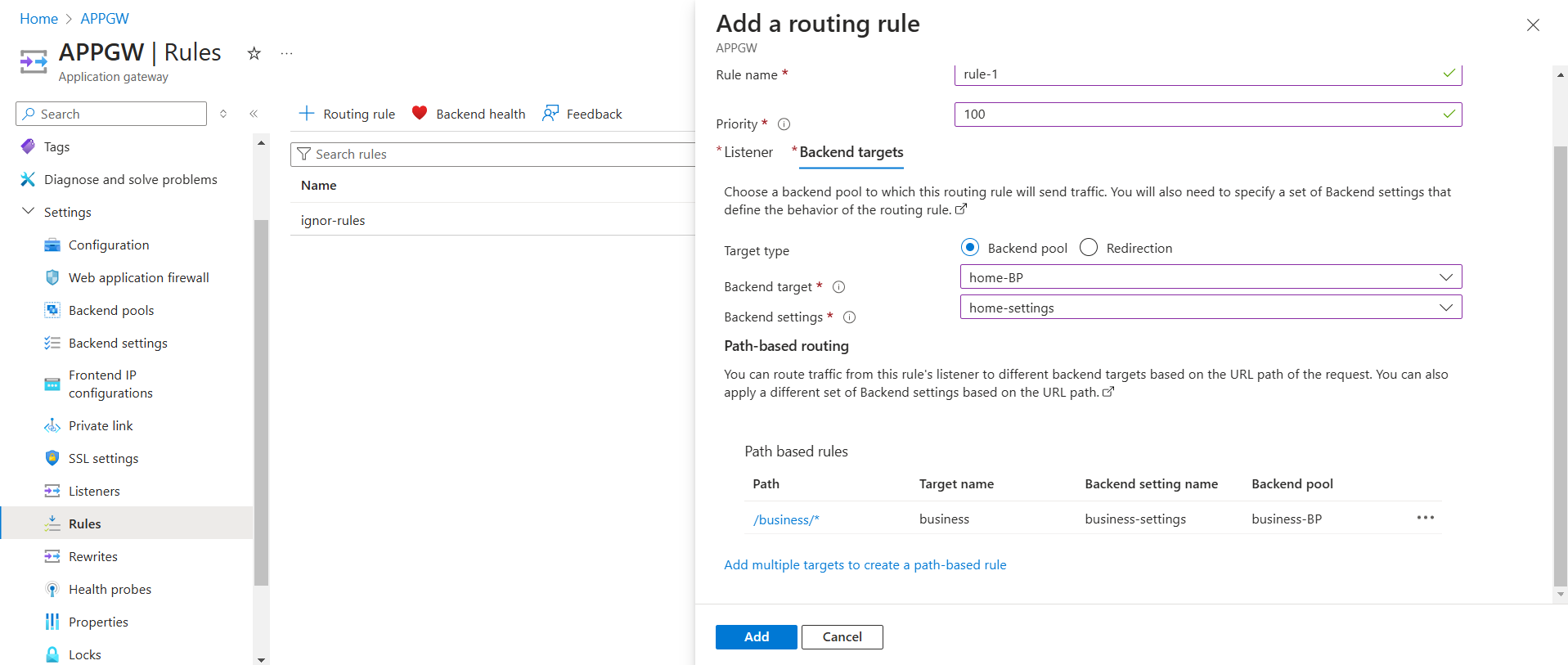


Fig: business health probe.

Case5: Adding the routing rules.



Step5: Using public IP of APPGW brows it in any browser (like 172.212.20.69 & 172.212.20.69/business).

