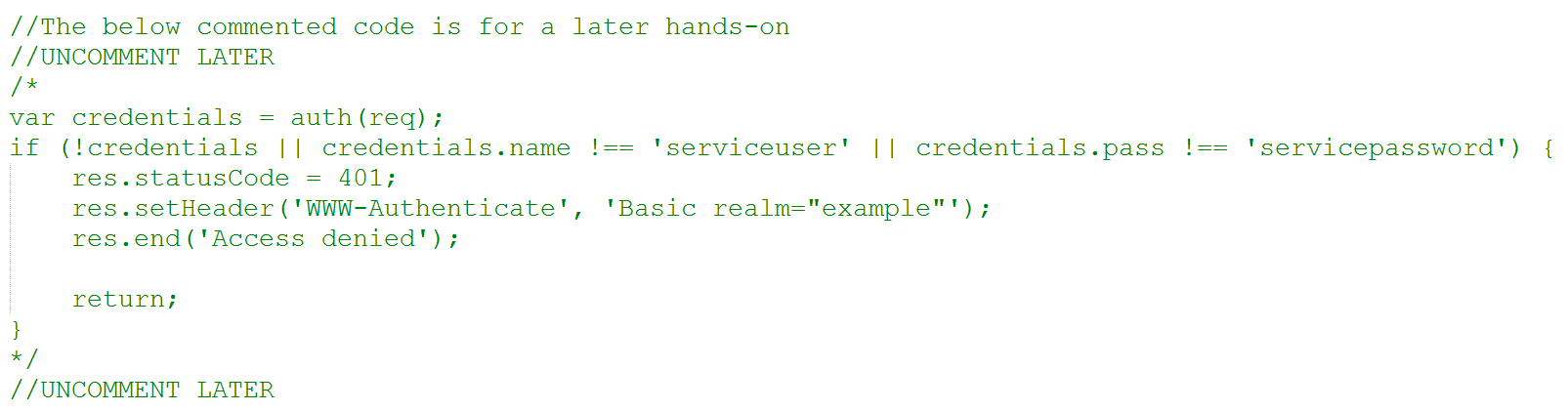
# Securing a Backend Service

## Configuring Basic Authentication

1. Open the server.js file of Product Assets service and uncomment the code within “UNCOMMENT LATER” section.

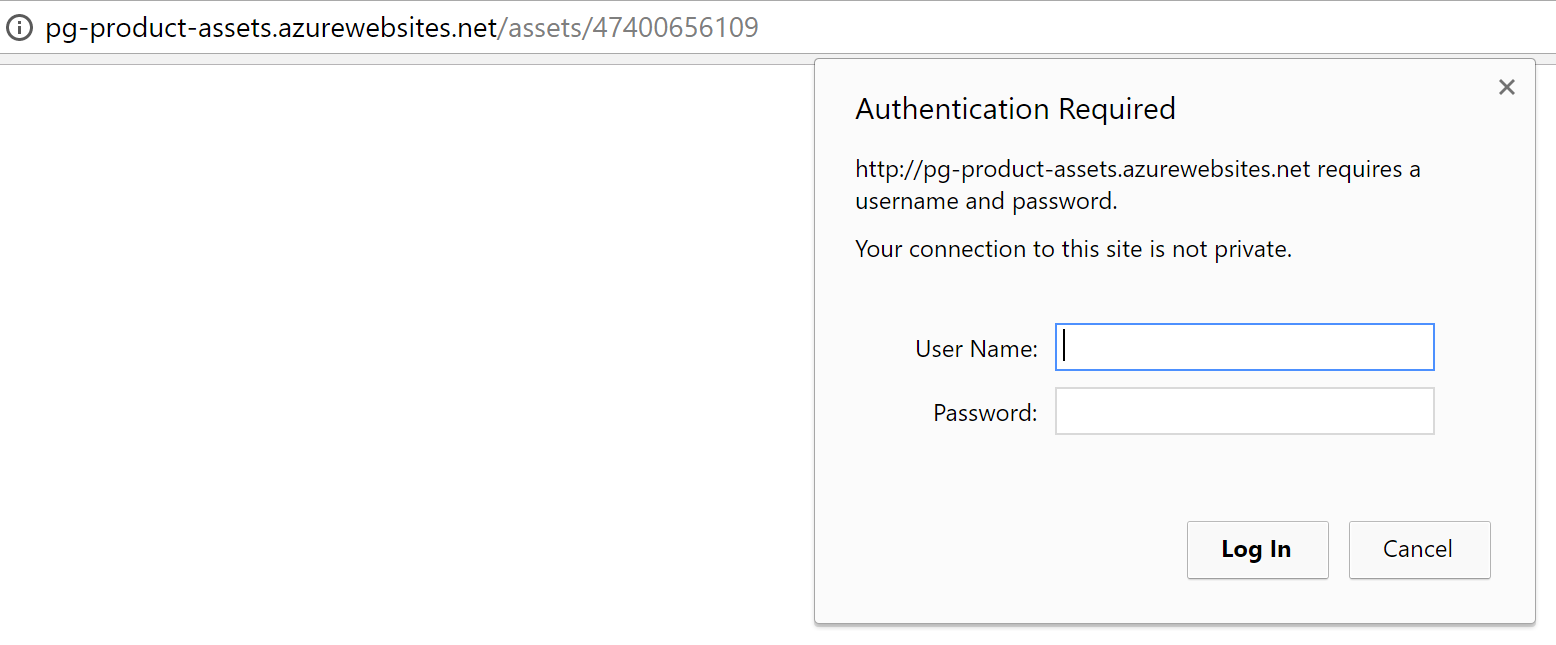


1. Understand the basic authentication code – not that the basic authentication username configured is “serviceuser” and password is “servicepassword”.
2. After the changes are done, run the following command to check-in the code.

**git commit -a -m “added basic auth security”**

**git push productassets master**

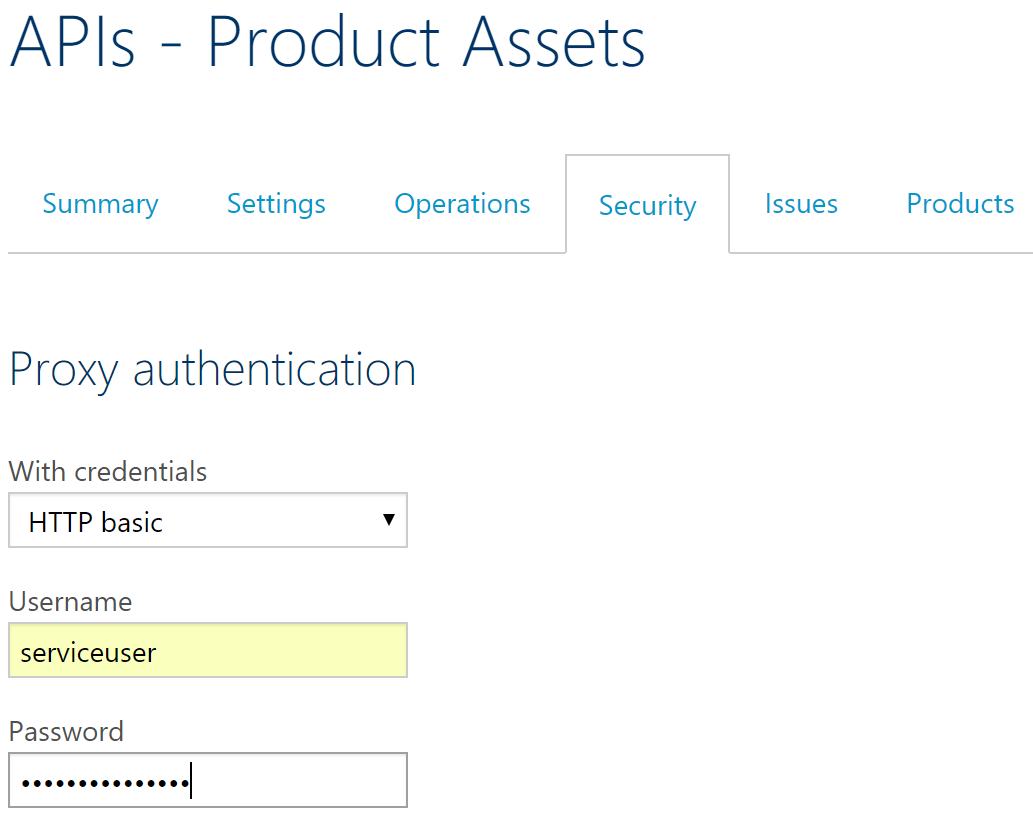
1. Wait for continuous deployment to Azure API App to complete
2. Access the Product Assets service – either the backend URL (<http://pg-product-assets.azurewebsites.net/assets/47400656109>) or the public URL configured in Azure API Management (<https://pgecommerce.azure-api.net/dam/assets/47400656109>). Note that there is an authentication dialog prompted now.



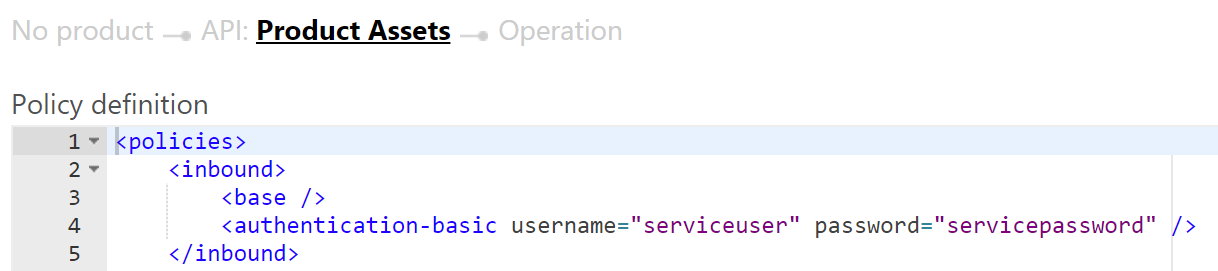
1. If credentials are not entered or incorrect credentials are entered, access to the service is denied.
2. Enter the right credentials (serviceuser / servicepassword) and the service returns results.

## Configuring Basic Authentication in API Management

1. Access the aggregated Products service (<https://pgecommerce.azure-api.net/products/47400656109>) and note that it throws a 404 error because of the error handling policy configured earlier.
2. Now go to Publisher Portal 🡪 APIs 🡪 Product Assets 🡪 Security and configure Proxy Authentication as shown below. This is for API Management to pass basic authentication credentials to the backend service.

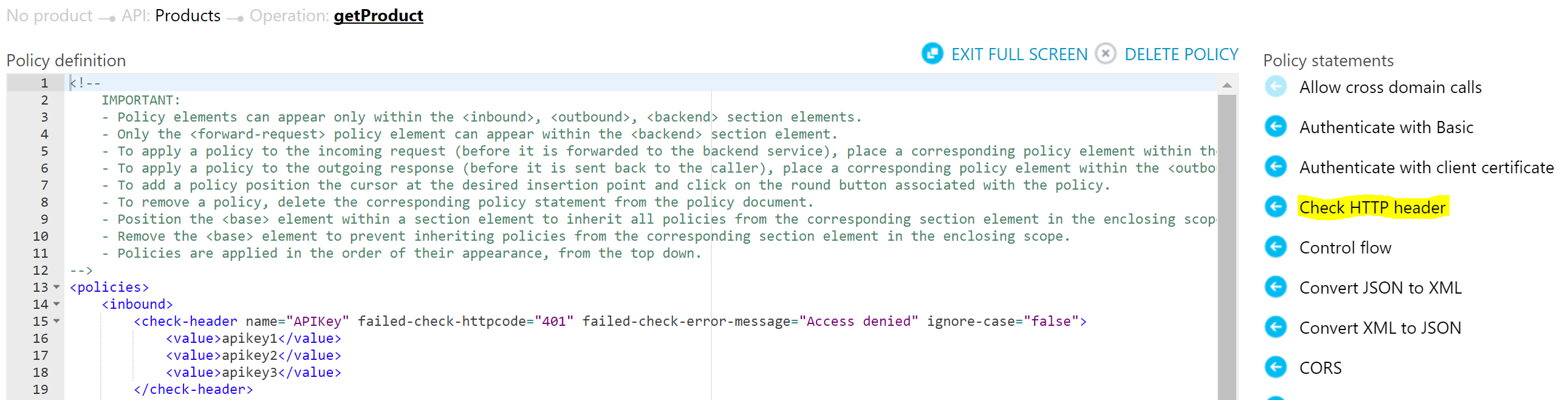


1. Access the aggregated Products service once again and note that it returns results without any prompt for credentials.
2. Also note that the above configuration has automatically added the “Authenticate with Basic” policy to the inbound section of the Product Assets service.



# Securing A Service with API Key

1. Go to the policy editor of the **getProduct** operation of Products API.
2. Add the “Check HTTP Header” policy to the inbound section of the service and configure it as shown below.



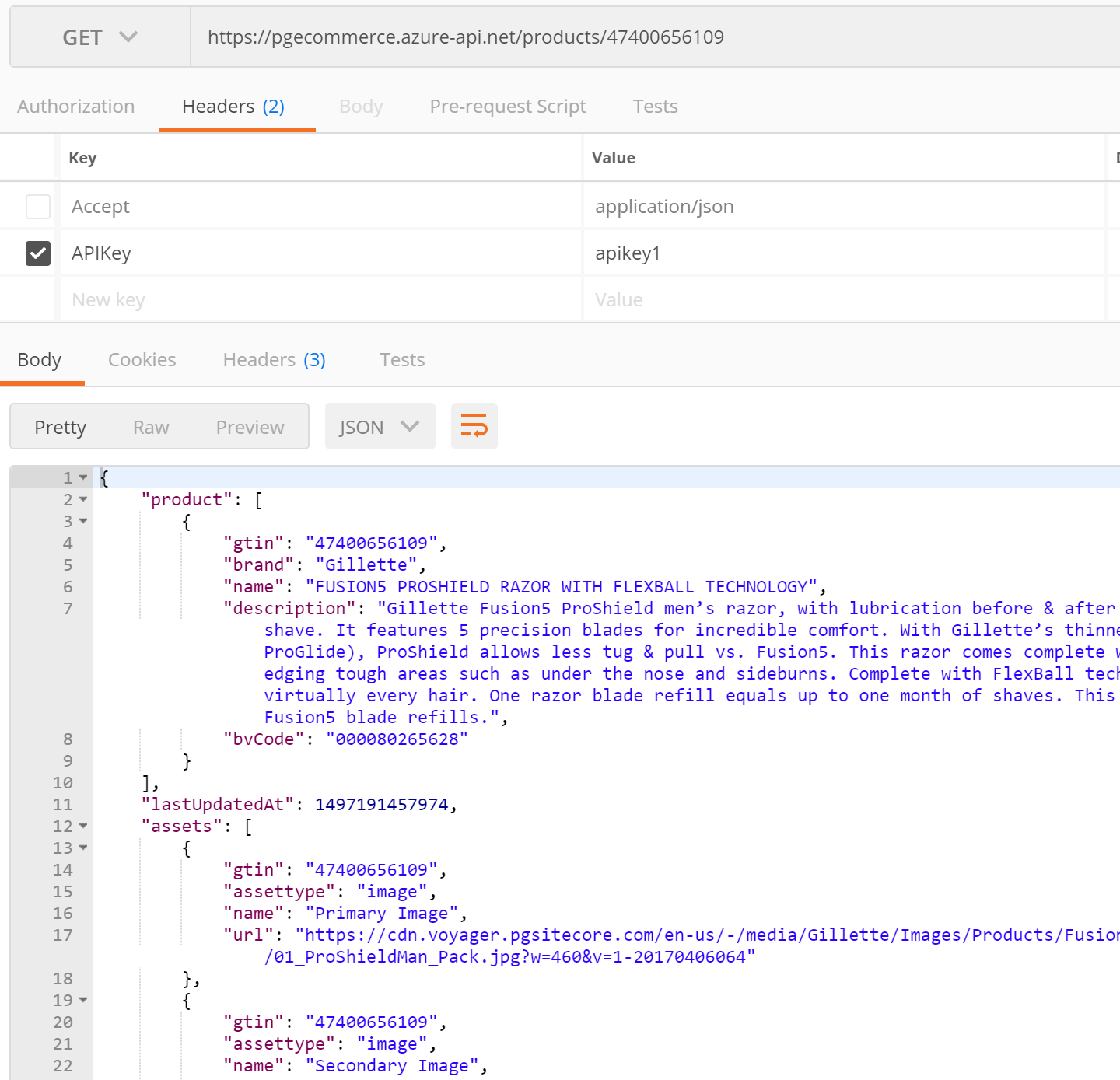
Alternatively copy the code in the attached file to the beginning of the inbound section of the policy.



1. The above policy ensures that the service can be accessed only if the request has an APIKey header with value being one of the values configured.
2. Access the Products service (<https://pgecommerce.azure-api.net/products/47400656109>) from a browser and note that it returns a 404 error.

*Note: in ideal scenario, it would have thrown a 401 Unauthorized error, but the error policy configured in earlier hands-on masks the 401 error with a 404 error. Alternatively, comment the on-error section in the policy to see the actual HTTP error message and status.*

1. Open Postman and configure APIKey HTTP header with one of the values configure in the policy – as shown below. Access the service now and the service now returns results.

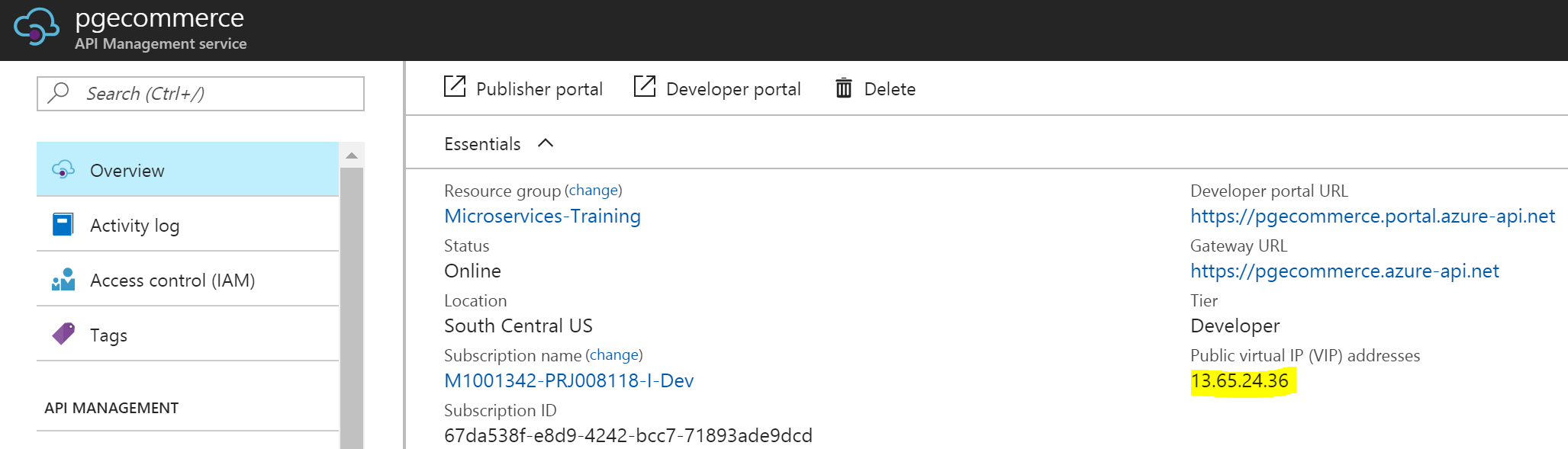


1. Comment out or delete the policy that was just configured – this is in preparation for the remaining hands-on.

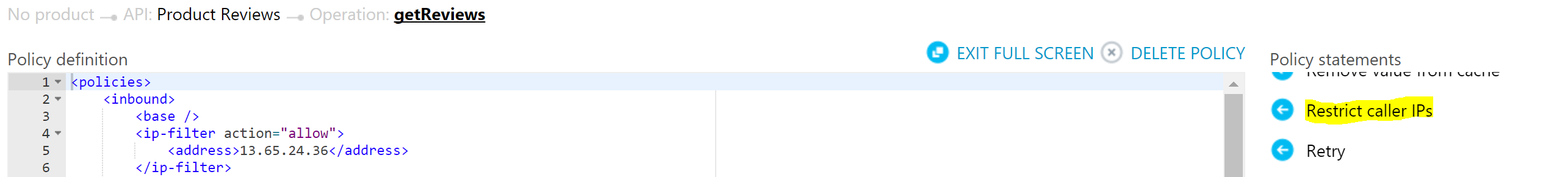
# Restrict Caller IPs

In this exercise, access to one of the services configured in Azure API Management will be restricted to only the Virtual IP of the API Gateway. This is to restrict anyone from directly accessing the service from the internet.

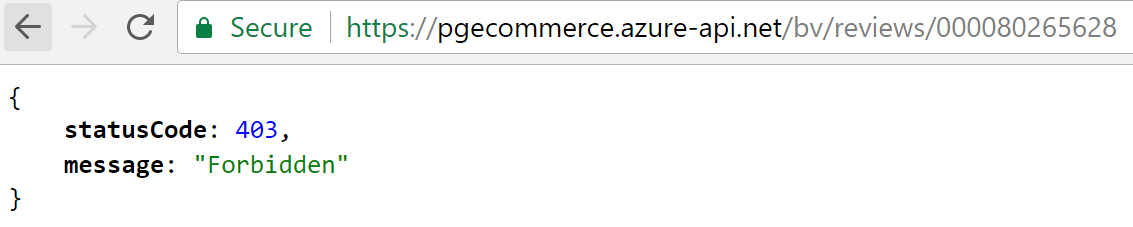
1. In the Azure Portal, go to API Management service and note down the public virtual IP of the API Gateway.



1. Go to policy editor of the **getReviews** operation of Product Reviews service.
2. Add the “Restrict caller IPs” policy to the inbound section of the service and configure it as shown below. The IP address entered should be the one noted in the earlier step.



1. Access the Product Reviews service (<https://pgecommerce.azure-api.net/bv/reviews/000080265628>) directly from a browser, and note that the 403 Forbidden error is returned as shown below.



1. However, when the aggregated Products service (<https://pgecommerce.azure-api.net/products/47400656109>) is accessed, it returns results including product reviews.

# References

* Access restriction policies – <https://docs.microsoft.com/en-us/azure/api-management/api-management-access-restriction-policies>