# These are suggested changes for the Infrastructure and Application Security Workshop: <https://github.com/CloudLabsAI-Azure/CAF-Infra-Security/blob/main/01-secure-administration-and-management.md>

# Exercise 2 - Secure administration and management

## Task 1: Network Health

Step 7: Update with correct screen shot that shows throughput.

A screenshot of a computer

Description automatically generated

## Task 2: Network Topology

### Add a step between 2 & 3:

On the topology page click on the bar to go to the new Topology experience:

A screenshot of a computer

Description automatically generated

# Exercise 3- Secure application

## Task 2: Accessing your application using application gateway

### Change the sentence that is before step 1 to:

In this task you will access the application by going through the Application Gateway that you just configured.

## Task 3:

### Change the sentence that is before step 1 to:

In this task, you will block access from the Lab VM to the Jump VM by configuring a Firewall Policy custom rule. The rule will deny access to the web application by adding the Lab VM’s Public IP in the deny rule.

### Step 12: Add this to the end of the step.

Note: This may take a few minutes to take effect.

## Task 4: Attack Simulation

### Add the following to the beginning of the task, before step 1:

Since we are already blocking the Public IP of the Lab VM from accessing the web application. You will want to perform this test from your own machine’s browser.

### Step 1: Change to the following text:

From your own machines browser, access the application by putting in the **Application Gateway IP** that you looked up in Task 2.

**Note**: Your browsing URL value should look like <http://20.185.224.102>

Now pass the value ?q=<script> at the end of your **Application Gateway** IP and try browsing it again. You can observe that the web application is accessible.

**Note**: Your browsing URL value should look like http://20.185.224.102/?q=<script>

## Task 5.3: Create a Rate Limit Rule:

### **Step 8: Change the first sentence from “In Conditions, enter the information required to specify a match condition to identify requests where the URL contains the string /promo:” to the following:**

**In Conditions, enter the information required to specify a match condition to identify requests where the URL contains the string ‘contoso’ and ‘azurefd’:**

### Step 11: Add the following:

Note: It may take a few minutes for the rate limit test policy to become active. Feel free to move on and come back later to test.

# Exercise 4 - Secure Infrastructure with Azure Firewall Premium

## Task 3:

### Step 17: Add to the instructions:

If you have trouble reaching www.nfl.com, try [www.nba.com](http://www.nba.com) or [www.nhl.com](http://www.nhl.com).