Barracuda Web Application Firewall

Reprovision a Virtual Machine Deployed on Cloud

The Barracuda Web Application Firewall virtual machine deployed on Microsoft Azure/Amazon Web Services can be reprovisioned using the web interface (called as WebConsconf).

Pre-requisites

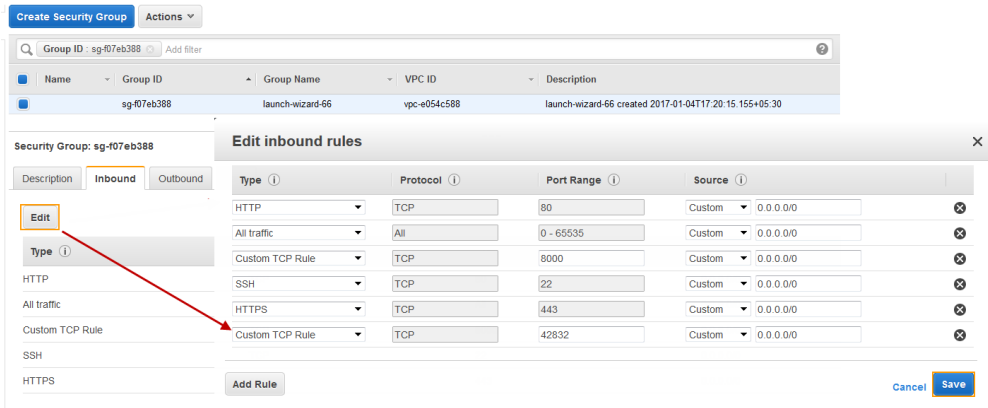The Barracuda Web Application Firewall virtual machine:

- Should have internet access to reach the Barracuda servers on port 80 and 443.
- Should not be clustered with other Barracuda Web Application Firewall virtual machine(s).
- Should have port 42832 opened in the Network Security Group on Microsoft Azure or Security Group on Amazon Web Services (Refer to the sections mentioned below).
    - [Configuring the WebConsConf Port for the Barracuda Web Application Firewall VM on Amazon Web Services](#)
    - [Configuring the WebConsConf Port for the Barracuda Web Application Firewall VM on Microsoft Azure](#)

Configuring the WebConsConf Port for the Barracuda Web Application Firewall VM on Amazon Web Services

1. Log into the [EC2 Management Console](#).
2. From the EC2 dashboard, select **Instances** under **INSTANCES**.
3. Select the instance that needs reprovisioning from the instances table.
4. Click on the security group in the **Description** tab. Also, note down the **Public DNS (IPv4)** or **IPv4 Public IP**.
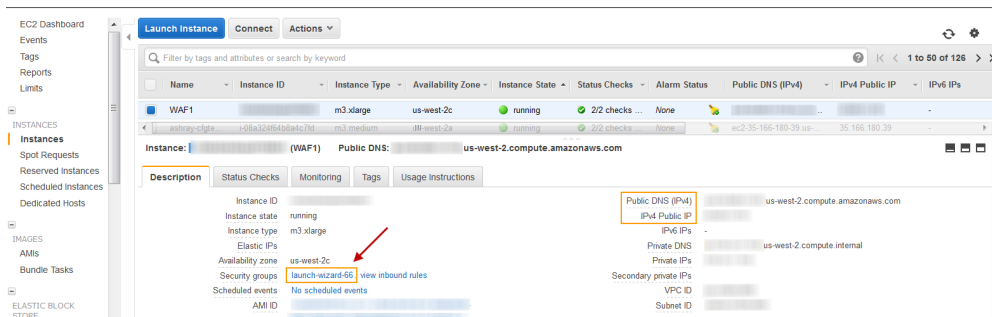

5. In the Security Group page, select the **Inbound** tab and click **Edit**.
6. In the **Edit inbound rules** window, click **Add Rule** and do the following:
    1. **Type**: Select *Custom TCP Rule*.
    2. **Port Range**: Specify *42832*.
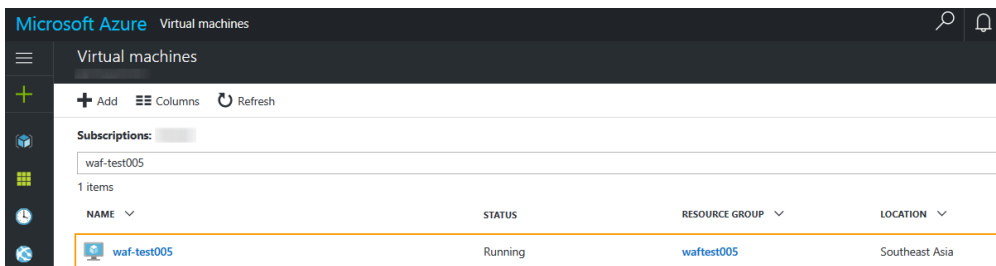   3. **Source**: Enter *0.0.0.0/0*
7. Click **Save**.

Barracuda Web Application Firewall

Configuring the WebConsConf Port for the Barracuda Web Application Firewall VM on Microsoft Azure
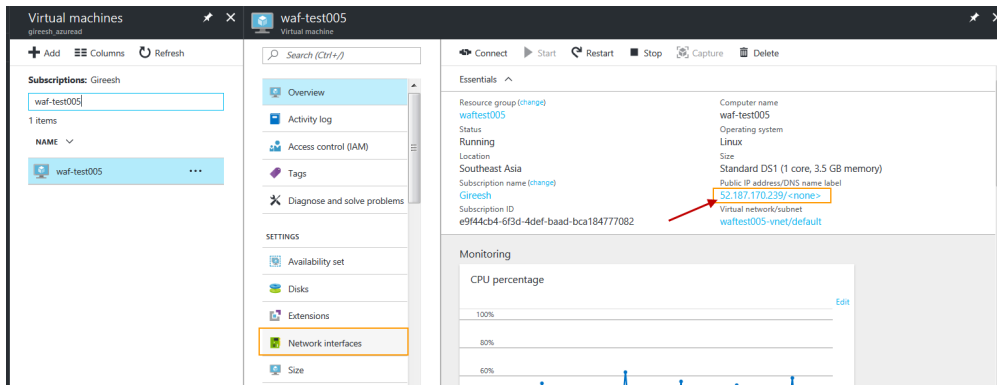
1. Log into the [Microsoft Azure Management Portal](#).
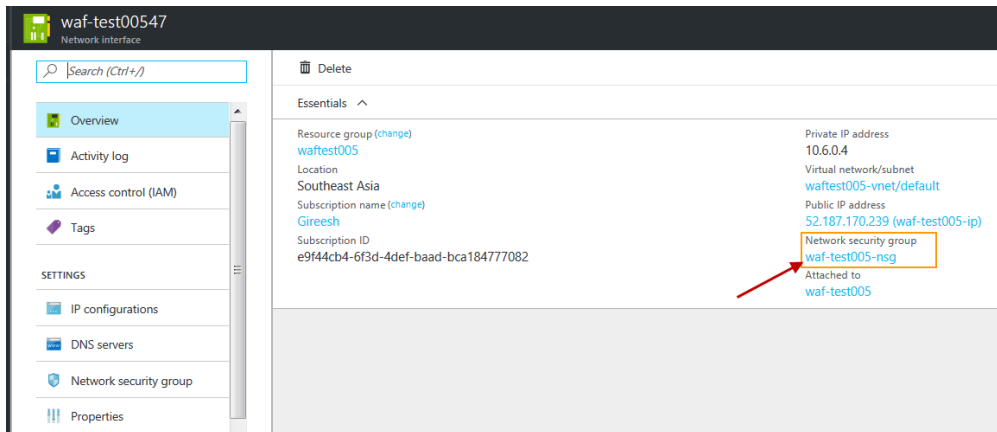2. Click **Virtual machines** on the left panel.
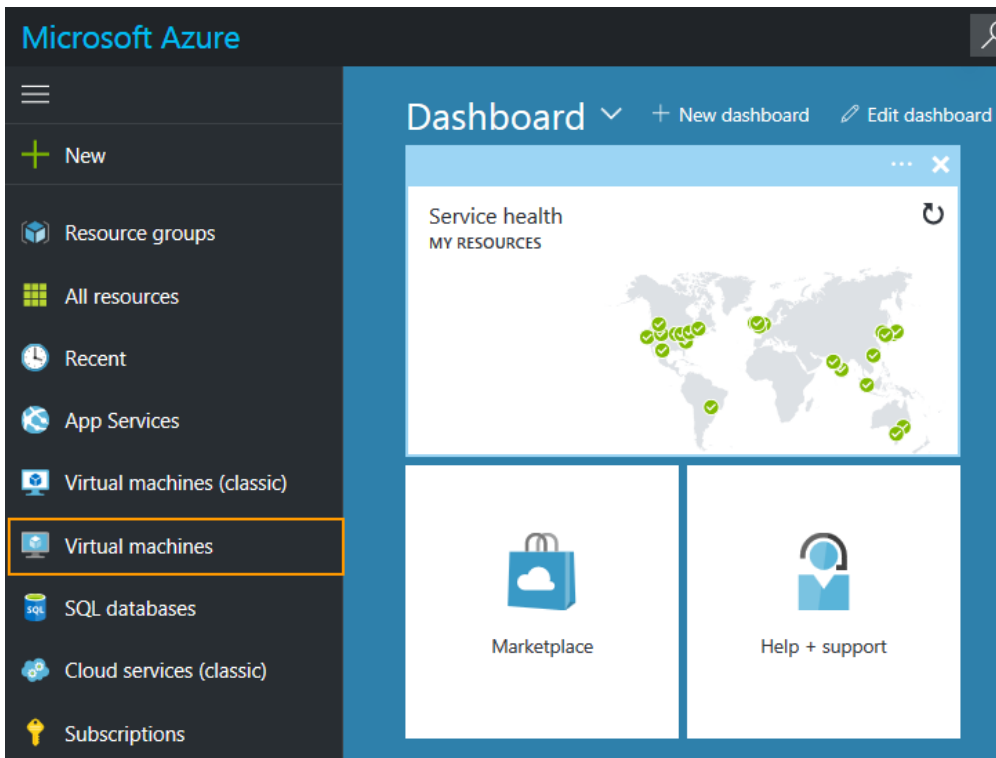
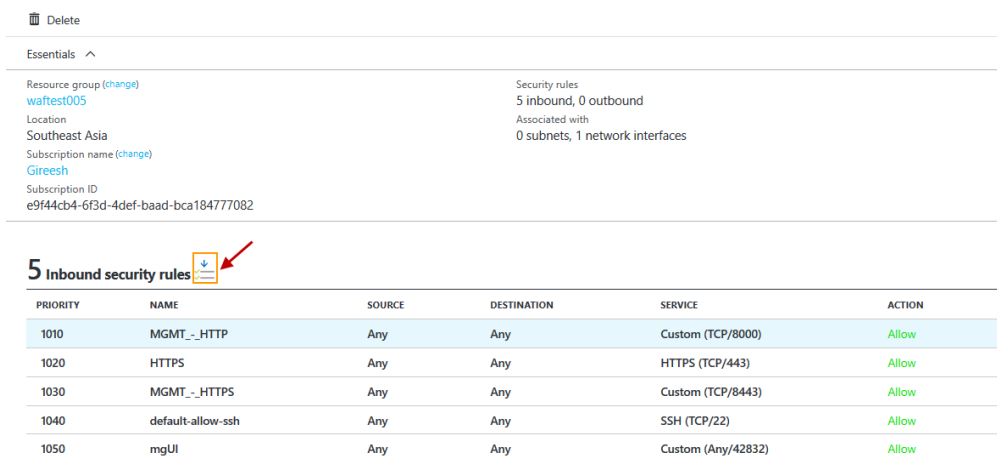3. In the **Virtual machines** page, locate the virtual machine that you want to reprovision.

4. Click on the instance, and select **Network Interfaces**. Also, jot down the **Public IP address/DNS server label** of the Barracuda Web Application Firewall instance.

5. Click on the network interface, and select the **Network security group** associated with the interface.

6. In the **Network security group** page, click on the icon next to **Inbound security rules**.


PRIORITY	NAME	SOURCE	DESTINATION	SERVICE	ACTION
1010	MGMT_-_HTTP	Any	Any	Custom (TCP/8000)	Allow
1020	HTTPS	Any	Any	HTTPS (TCP/443)	Allow
1030	MGMT_-_HTTPS	Any	Any	Custom (TCP/8443)	Allow
1040	default-allow-ssh	Any	Any	SSH (TCP/22)	Allow
1050	mgUI	Any	Any	Custom (Any/42832)	Allow

7. In the **Inbound security rules** page, click **Add**.
8. In the **Add Inbound security rule** page, do the following:
    1. **Advanced**: Enter a name.
    2. **Priority**: Set the priority order for the rule.
    3. **Source**: Any
    4. **Service**: Custom
    5. **Protocol**: Any
    6. **Port range**: 42832
    7. **Action**: Allow
9. Click **OK**.

Barracuda Web Application Firewall
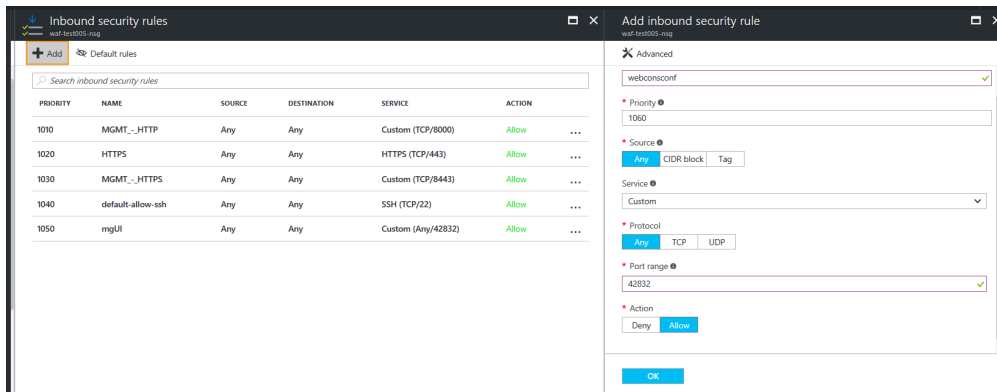
Reprovisioning the Barracuda Web Application Firewall virtual machine deployed on Microsoft Azure/Amazon Web Services

Perform the steps below to reprovision the Barracuda Web Application Firewall virtual machine (VM):

1. Open a web browser, and enter the public IP address followed by the port jotted down in the **Configuring the WebConsConf Port for the Barracuda Web Application Firewall VM on Microsoft Azure/Amazon Web Services** section.
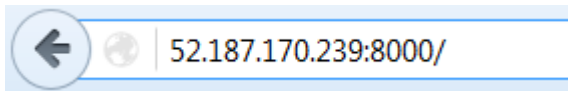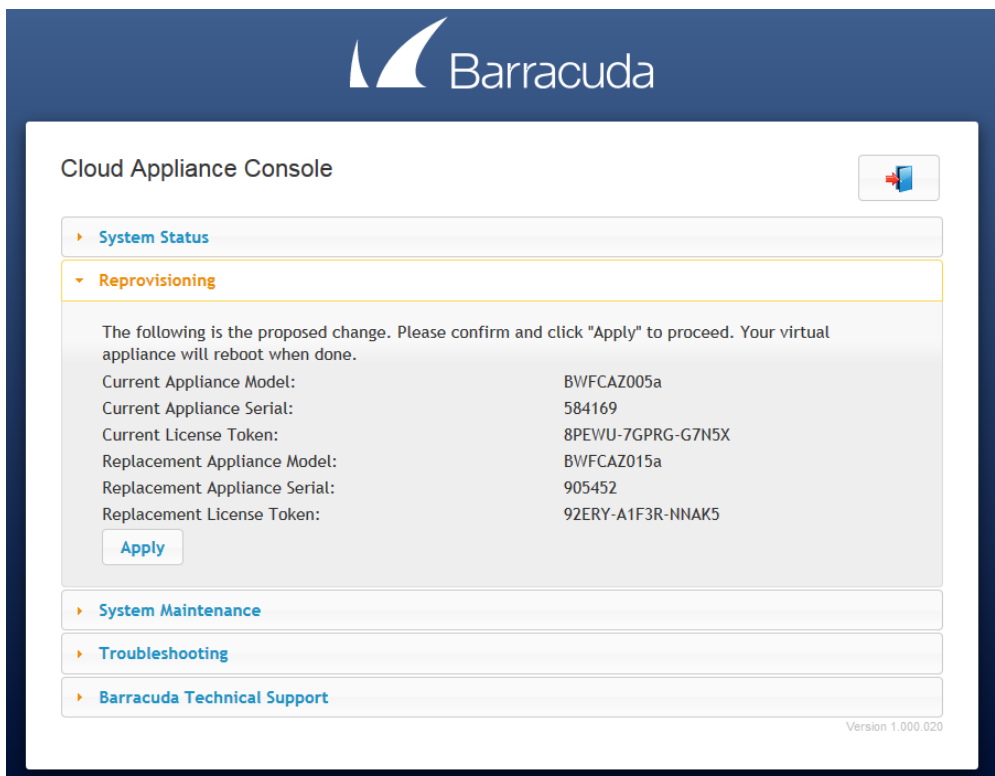

2. Log into the Barracuda Web Application Firewall web interface using the credentials.
3. Go to the **NETWORKS > ACL** page, **Auto Created System ACLs** section and check if the web consconf rule is created with port 42832.
4. Now, open another web browser and enter the public IP address jotted down in step **4**, followed by the web consconf port (42832).
5. Log into the Cloud Appliance Console using your *admin* user credentials.

6. In the **Cloud Appliance Console** page, click **Reprovisioning** and do the following:
   1. Enter the new license key in the **Replacement License Token** text box.
   2. Click **Download**.
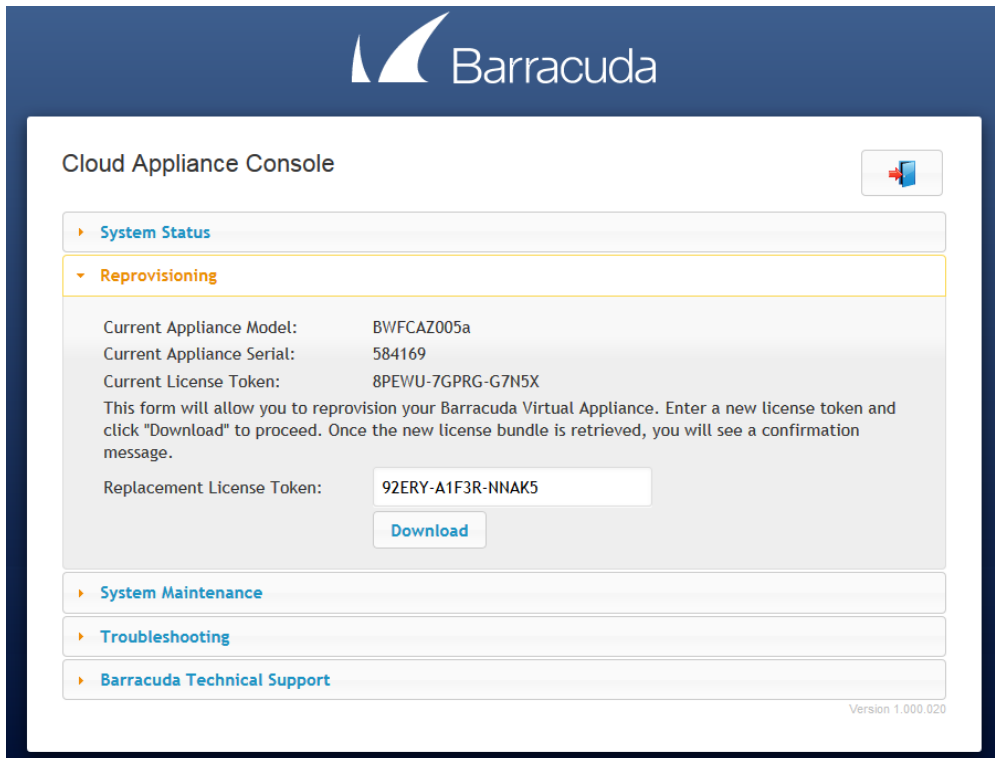
3. After the download is complete, click **Apply**.

7. The Barracuda Web Application Firewall virtual appliance gets provisioned with the new model and serial number.

8. The virtual appliance reboots with the new serial number and the selected model.

Figures