Load Balancing For Clustered Barracuda Web Application Firewall Instances in the Old Microsoft Azure Management Portal

https://campus.barracuda.com/doc/41094180/

This guide will walk you through the steps to load balance traffic across multiple instances of the Barracuda Web Application Firewall deployed in the old Microsoft Azure Management Portal.

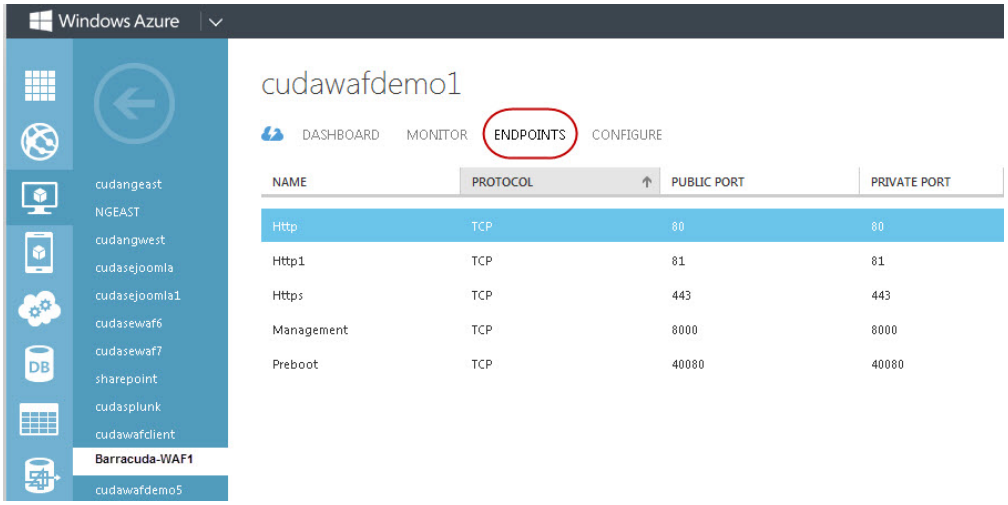
> In Microsoft Azure, you can create Services using the **WAN IP Address** of the Barracuda Web Application Firewall.

To configure a load-balanced set in the old Microsoft Azure Management Portal, do the following:

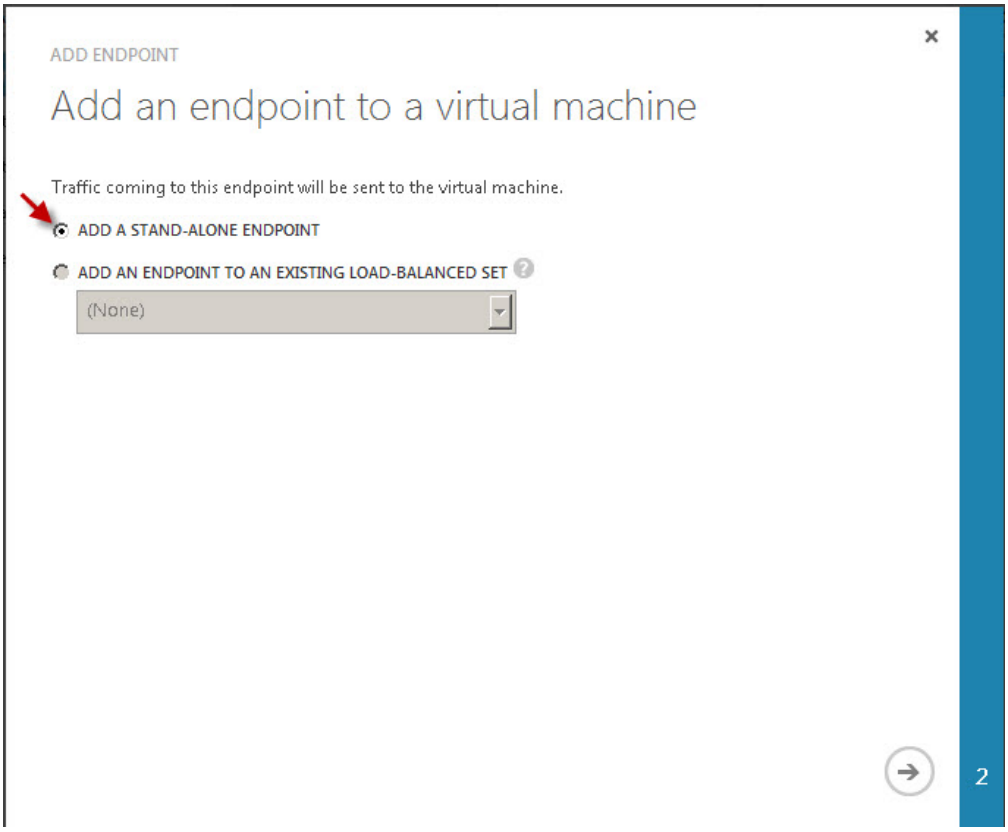
Complete the steps in Step 1. Deploy the Barracuda Web Application Firewall Instances in Microsoft Azure and Step 2. Set Up a High Availability Environment With the Barracuda Web Application Firewall under the **Configuring a Load-Balanced Set Using the Classic Model** section**,** and proceed with the steps below:

Step 3. Set Up Load Balancing on the First Barracuda Web Application Firewall Instance

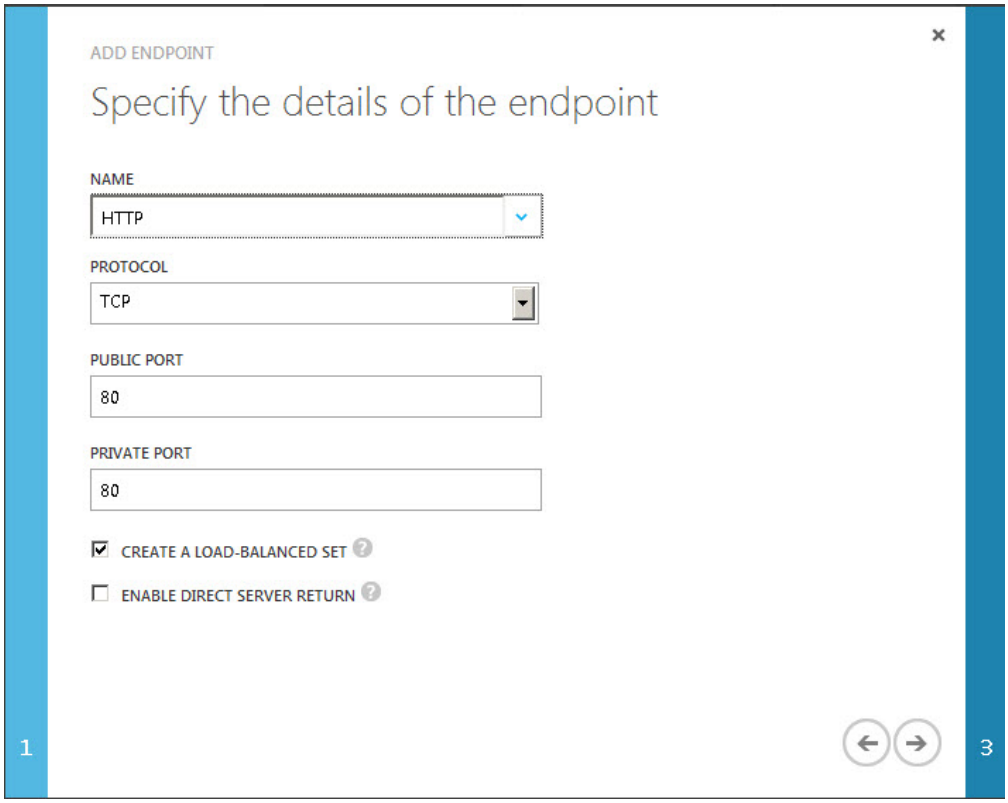
1. Go to the Microsoft Azure Management Portal.
2. Click **Virtual Machines** and select *Barracuda-WAF1*.
3. Click **ENDPOINTS,** and then click **ADD**.



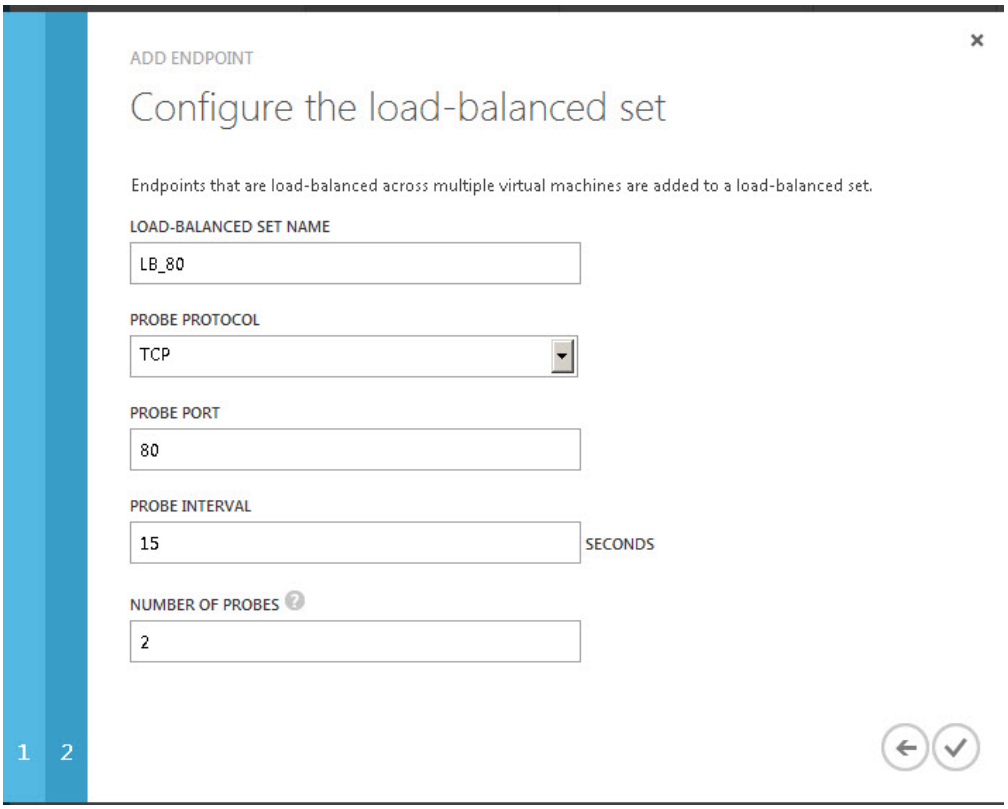
4. In the **Add an endpoint to a virtual machine** window, select **Add A STAND-ALONE ENDPOINT** and click the arrow to continue.



5. Specify values for the following fields:
    1. **NAME** – Enter the name for the endpoint. **Example**: HTTP
    2. **PROTOCOL** – Select **TCP** from the list.
    3. **PUBLIC PORT** – Enter the port number of the service you are load balancing. **Example**: Port 80 for HTTP traffic.
    4. **PRIVATE PORT** – Enter the internal port that should listen to traffic on the endpoint. **Example**: 80.
    5. Select **Create A LOAD-BALANCED SET** and click the arrow to continue.



6. In the **Configure the load-balanced set** window, specify a name for the load-balanced set and assign the values for the load-balancing probe.



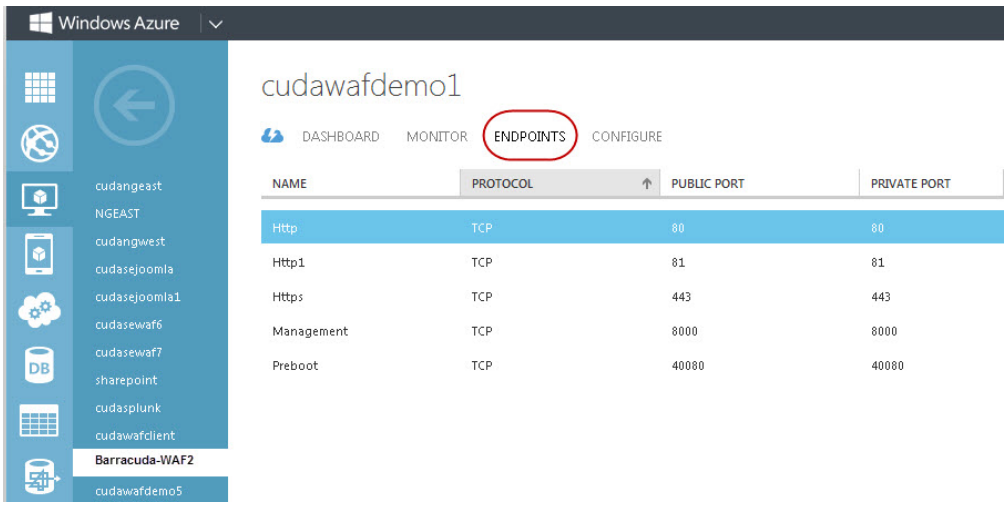
7. Click the check mark to set up a load-balanced set.

8. Repeat the process to add more ports to the load-balanced set.

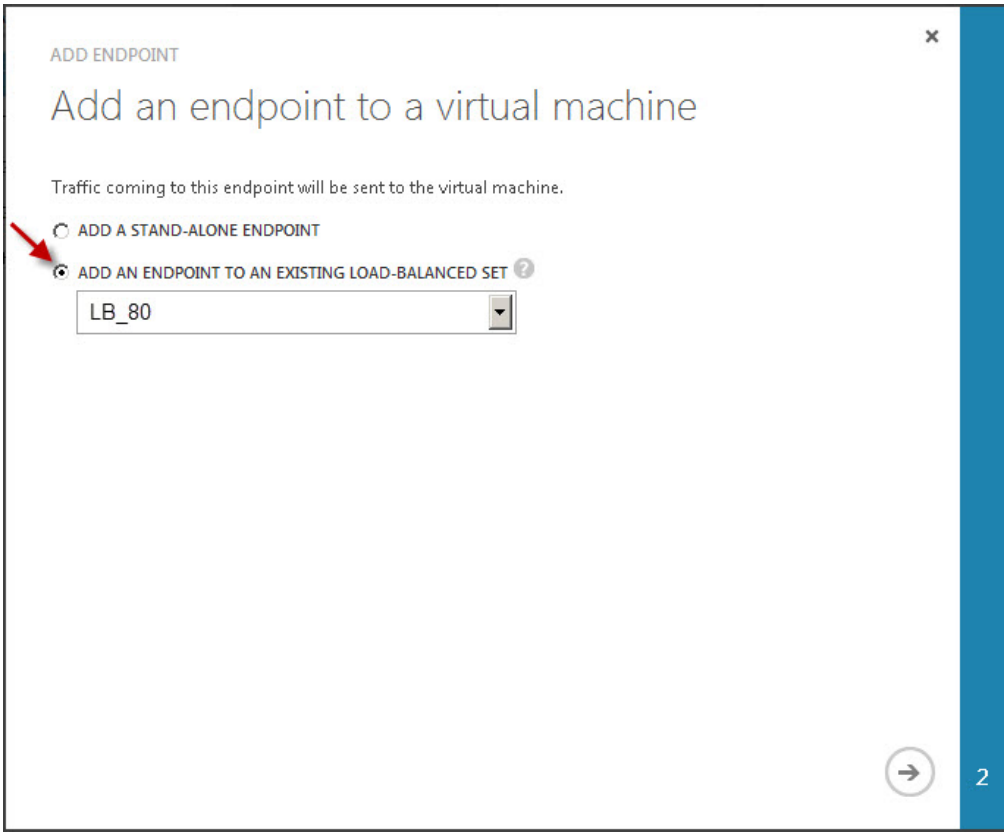
Step 4. Add Other Barracuda Web Application Firewall Instances to the Load-Balanced Set

After you create the load-balanced set for Barracuda-WAF1, add other Barracuda Web Application Firewall virtual machines to the set. **Example**: Barracuda-WAF2

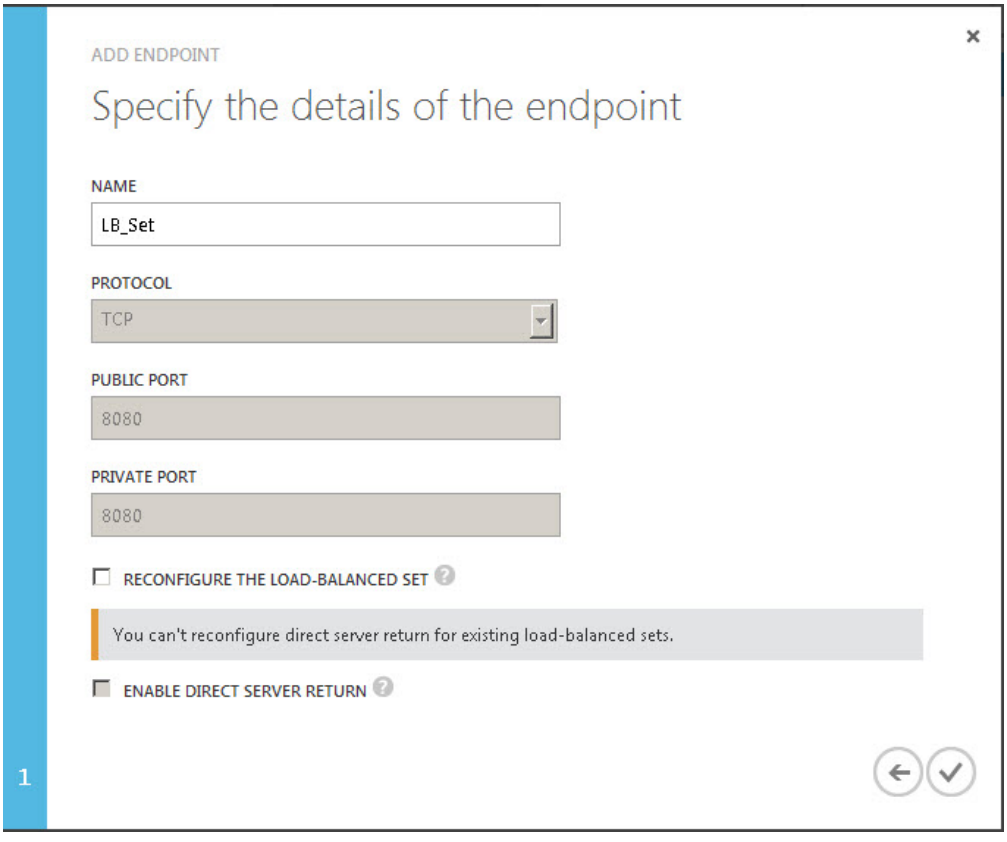
1. Go to the Microsoft Azure Management Portal.
2. Click **Virtual Machines** and select *Barracuda-WAF2*.
3. Click **ENDPOINTS**, and then click **ADD**.



4. In the **ADD ENDPOINT** window, select **ADD AN ENDPOINT TO AN EXISTING LOAD-BALANCED SET** and then select the load-balanced set name from the list. Click the arrow to continue.



5. In the **Specify the details of the endpoint** window, specify a name for the load-balanced set and then click the check mark.



6. Repeat the process to add more Barracuda Web Application Firewall virtual machines to the load-balanced set.

Figures

1. ENDPOINT.jpg
2. ENDPOINTS_1.jpg
3. ENDPOINT_2.jpg
4. ENDPOINT_3.jpg
5. lb.jpg
6. lb_1.jpg
7. lb_2.jpg

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.