# 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
  - <u>Configuring the WebConsConf Port for the Barracuda Web Application Firewall VM on Microsoft</u> <u>Azure</u>

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

- 1. Log into the <u>EC2 Management Console</u>.
- 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**.

EC2 Dashboard	↓ Launch Instance Connect Actions Y	0 Ø	
Tags	Q. Filter by tags and attributes or search by keyword @ K < 11	to 50 of 126	×
Reports Limits	Name v Instance ID v Instance Type v Availability Zone v Instance State A Status Checks v Alarm Status Public DNS (IPv4) v IPv4 Public IP v	IPv6 IPs	
=	WAF1 m3.xlarge us-west-2c		
STANCES	< 👔 ashray-cfgte i-08a324f64b8a4c7fd m3.medium UBF-west-2a 🥥 running 🥏 2/2 checks None 🍡 ec2-35-166-180-39.us 35.166.180.39		Þ.
nstances	Instance: (WAF1) Public DNS: us-west-2.compute.amazonaws.com		5
pot Requests			
Reserved Instances	Description Status Checks Monitoring Tags Usage instructions		
cheduled Instances			
edicated Hosts	instance ID Public DNS (IP-44) us-west-2.compute.amazonaws.com		
	instance state running		
GES	Instance type m3.xlarge IP-V6 IP-9 -		
dis	Elastic IPs Private DNS us-west-2 compute internal		
indie Tasks	Availability zone us-west-2c Private IPs		
	Security groups launch-wizard-66 view inbound rules Secondary private IPs		
	Scheduled events VPC ID		
STIC BLOCK	AMI ID Subnet ID		

- 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

Group ID : sg-f07eb388 O Add filte				Θ
Name - Group ID	▲ Group Name	- VPC ID	- Description	
sg-f07eb388	launch-wizard-66	vpc-e054c588	launch-wizard-66 created 2	017-01-04T17:20:15.155+05:30
Security Group: sg-f07eb388	Edit inbound rules			
Description Inbound Outbourn	1 Туре (i)	Protocol (i)	Port Range ()	Source ①
Edit	НТТР	TCP	80	Custom 💌 0.0.0.0/0
	All traffic	All	0 - 65535	Custom • 0.0.0.0/0
Туре ()	Custom TCP Rule	TCP	8000	Custom • 0.0.0.0/0
нттр	SSH -	TCP	22	Custom • 0.0.0.0/0
All traffic	HTTPS -	TCP	443	Custom • 0.0.0.0/0
	· ·			

## 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.

Micro	DSOFT AZURE Virtual machines			٦ ب
≡	Virtual machines			
+	+ Add			
	Subscriptions:			
	waf-test005			
	1 items			
4	NAME Y	STATUS	RESOURCE GROUP $\checkmark$	location $\checkmark$
	👰 waf-test005	Running	waftest005	Southeast Asia

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.



gireesh_azuread	Wirtual machine	
+ Add ≣≣ Columns ひ Refresh		In Connect In Start I Restart I Stop I Capture
Subscriptions: Gireesh	Overview	Essentials ^
waf-test005		Resource group (change) Computer name waftest005 waf-test005
1 items	Activity log	Status Operating system
NAME V	Access control (IAM)	Running Linux
🚺 waf-test005 🚥	🛷 Tags	Succession Size Southeast Asia Standard DS1 (1 core, 3.5 GB memory) Solution Standard DS1 (1 core, 3.5 GB memory)
	X Diagnose and solve problems	Subscription name (unamper) Public in address/UNS name label Gireesh Subscription ID Visitian antwork/subset
	SETTINGS	e9/44cb4-6/3d-4def-baad-bca184777082 waftest005-vnet/default
	Availability set	Monitoring
	😕 Disks	CPU percentage
	Extensions	100% Edit
	Network interfaces	80%

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

waf-test00547			
Search (Ctrl+/)		Delete	
Overview	<u>^</u>	Essentials ^	0
Activity log		waftest005	10.6.0.4
Access control (IAM)		Location Southeast Asia	Virtual network/subnet waftest005-vnet/default
Tags		Subscription name ( <del>change</del> ) Gireesh	Public IP address 52.187.170.239 (waf-test005-ip)
	=	Subscription ID e9f44cb4-6f3d-4def-baad-bca184777082	Network security group waf-test005-nsg
SETTINGS	_		Attached to waf-test005
IP configurations	_		
DNS servers			
Network security group			
Properties			

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

Delete					
Essentials ^					
Resource group (ch waftest005 Location Southeast Asia Subscription name Gireesh Subscription ID e9f44cb4-6f3d-4	ange) (change) Idef-baad-bca184777082		Security rules 5 inbound, 0 o Associated with 0 subnets, 1 ne	utbound twork interfaces	
5 Inbound se	ecurity rules				
PRIORITY	NAME	SOURCE	DESTINATION	SERVICE	ACTION
1010	MGMTHTTP	Any	Any	Custom (TCP/8000)	Allow
1020	HTTPS	Any	Any	HTTPS (TCP/443)	Allow
1030	MGMTHTTPS	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

○ Search ini	bound security rules					webconsconf
PRIORITY	NAME	SOURCE	DESTINATION	SERVICE	ACTION	* Priority ©
1010	MGMTHTTP	Any	Any	Custom (TCP/8000)	Allow	 1050
1020	HTTPS	Any	Any	HTTPS (TCP/443)	Allow	 Any CIDR block Tag
1030	MGMTHTTPS	Any	Any	Custom (TCP/8443)	Allow	 Service
1040	default-allow-ssh	Any	Any	SSH (TCP/22)	Allow	 Custom
1050	mgUI	Any	Any	Custom (Any/42832)	Allow	 * Protocol
						Any ICP ODP
						42832
						* Action

## 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.

<ul> <li>€ € 52.187.170.239:42832</li> </ul>		C Q Search	☆│自	•
				C
		_		
	L Barracud	3		
Cloud Applian	e Console			
Username:	username			
Password:	password			
Login				

- 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.

lou	d Appliance Console		-
• 5	iystem Status		
₹ F	Reprovisioning		
	Current Appliance Model:	BWFCAZ005a	
(	Current Appliance Serial:	584169	
	Current License Token:	8PEWU-7GPRG-G7N5X	
	This form will allow you to repro click "Download" to proceed. On message.	vision your Barracuda Virtual Appliance. Enter a ce the new license bundle is retrieved, you will	a new license token and see a confirmation
	Replacement License Token:	92ERY-A1F3R-NNAK5	
		Download	
	System Maintenance		

3. After the download is complete, click **Apply**.

aud Appliance Console	
System Status	4
Reprovisioning	
The following is the proposed change. Pleas appliance will reboot when done.	e confirm and click "Apply" to proceed. Your virtual
Current Appliance Model:	BWFCAZ005a
Current Appliance Serial:	584169
Current License Token:	8PEWU-7GPRG-G7N5X
Replacement Appliance Model:	BWFCAZ015a
Replacement Appliance Serial:	905452
Replacement License Token:	92ERY-A1F3R-NNAK5
Apply	
System Maintenance	

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

К	arracuda
Cloud Appliance Console	
System Status	
- Reprovisioning	
Your Barracuda Virtual Appliance has successfully	been provisioned.
New Appliance Model:	BWFCAZ015a
New Serial Number:	905452
The Virtual Appliance is now rebooting.	
System Maintenance	
Troubleshooting	
Barracuda Technical Support	

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

	•
System Status	
Reprovisioning	
Current Appliance Model:	BWFCAZ015a
Current Appliance Serial:	905452
Current License Token:	92ERY-A1F3R-NNAK5
This form will allow you to re click "Download" to proceed. message.	provision your Barracuda Virtual Appliance. Enter a new license token and Once the new license bundle is retrieved, you will see a confirmation
Replacement License Token:	
	Download
System Maintenance	

Barracuda Web Application Firewall

