Public Cloud Hosting

https://campus.barracuda.com/doc/41115874/

The growth of cloud computing capabilities and services has driven more data into places where traditional IT security cannot reach - into the datacenters of public cloud providers. Cloud-based deployments can be in the form of a private cloud, where the Barracuda NG Firewall can act as a gateway device, or in a public or hybrid cloud. You can secure instances in a public or hybrid cloud by deploying a Barracuda NG Firewall as a virtual security device within your cloud environment. The Barracuda NG Firewall uses application and user awareness combined with advanced bandwidth management to optimize WAN performance and reliability, thereby securely handling all incoming traffic for the backend server instances.

Microsoft Azure Cloud

Microsoft Azure is a public cloud service. The Barracuda NG Firewall integrates into your Microsoft Azure virtual network by creating a network security gateway between Internet-facing endpoints and your virtual machines. Microsoft Azure **Small** and **Medium** instances use one virtual network interface with a dynamic IP address per virtual machine and can be deployed via web interface or a Microsoft PowerShell script. **Large** and **Extra Large** instances support two and four network interfaces, respectively, and must be deployed via PowerShell. The Barracuda NG Firewall Azure is available in four different sizes:

- **Level 2** – Small (1 core, 1.75 GB memory, one NIC)
- **Level 4** – Medium (2 cores, 3.5 GB memory, one NIC)
- **Level 6** – Large (4 cores, 7 GB memory, up to two NICs)
- **Level 8** – Extra Large (8 cores, 14 GB memory, up to four NICs)

To deploy a Barracuda NG Firewall in the Microsoft Azure Cloud via

- Web Interface, using only one network interface, see How to Deploy the Barracuda NG Firewall Azure on Microsoft Azure.
- PowerShell, using advanced networking features and, optionally, multiple network interfaces, see How to Deploy the Barracuda NG Firewall on Microsoft Azure via PowerShell.

Amazon Web Services (AWS)

Amazon AWS offers both virtual private and public cloud services. If you are deploying a virtual private cloud, the Barracuda NG Firewall AWS will act as a gateway device, just like in a traditional network. Internal IP addresses in the VPC can be static or dynamic; public IPs (Amazon Elastic IPs) are then mapped to the internal Network Interfaces. The AMI uses one dynamic Network Interface as a default configuration. Up to 9 additional Amazon Network Interfaces can be added, depending on the instance type with a total of up to 100 network interfaces per VPC. These network interfaces can be connected to subnets in the virtual private cloud, with each subnet containing server instances hosted in a different Availability Zone of your choice. The Barracuda NG Firewall AWS is available in four different sizes:

- **m3.small** – 1 vCPU core, up to two NICs, 4 IP addresses per interface
- **c1.medium** – 2 vCPU cores, up to three NICs, 10 IP addresses per interface
- **m3.xlarge** – 4 vCPU cores, up to three NICs, 10 IP addresses per interface
- **c1.xlarge** – 8 vCPU cores, up to four NICs, 15 IP addresses per interface

To deploy a Barracuda NG Firewall in an Amazon Virtual Private Cloud, see How to Deploy the Barracuda NG Firewall in an Amazon Virtual Private Cloud.

Figures

1. CloudNGs.png