Cloud Integration

https://campus.barracuda.com/doc/79463429/

To use your CloudGen Firewall in Azure or AWS to its fullest extent, the firewall must be configured to allow it to connect to the underlying cloud fabric. Using REST API calls, the firewall retrieves platform-specific data, or connects to other cloud services.

Azure Cloud Integration

Azure Cloud integration allows the firewall to rewrite Azure User Defined Routes and to monitor the IP Forwarding setting of the NIC of your firewall VM. Azure User Defined Routing allows you to use the CloudGen Firewall high availability cluster in the public subnet as the default gateway for all your VMs running in the backend networks.

For more information, see Cloud Integration for Azure.

AWS Cloud Integration

The IAM role assigned to the CloudGen Firewall instance allows the firewall access to the required AWS cloud service APIs. Depending on the use case, and how the CloudGen Firewall is deployed in AWS, access to various AWS services may be needed.

For more information, see Cloud Integration for AWS.

Cloud Best Practice

Due to the limitations imposed by the cloud platforms on the firewall, services must be configured to use a listener on a 127.0.0.X IP address. Traffic is forwarded to the service using application redirect rules.

For more information, see Best Practice - Service Configurations in the Public Cloud.