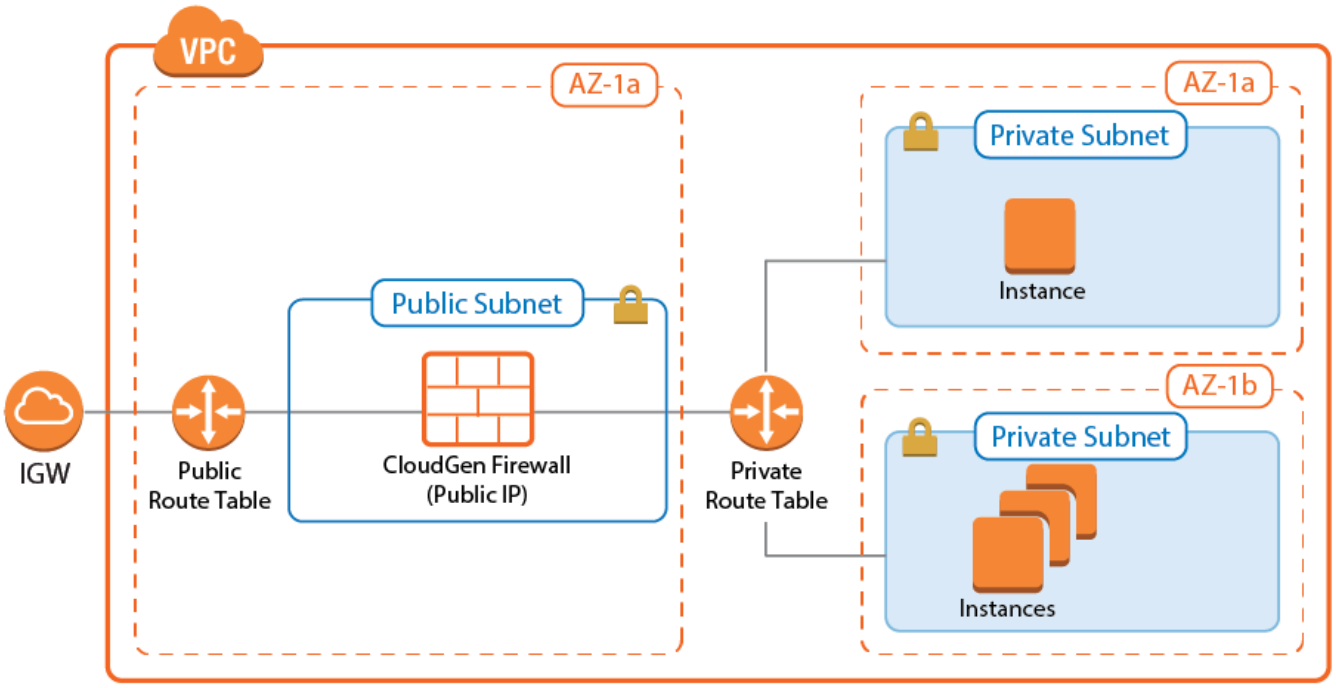
Amazon AWS Deployment

https://campus.barracuda.com/doc/96026603/

The CloudGen Firewall can secure your AWS resources and connect them to your on-premises network. The firewall VM replaces both the NAT gateway instances and the AWS VPN gateway with one single product. Using a firewall instead of the built-in security features of the AWS VPC allows for traffic visibility and more granular security policies, as well as central management using a Barracuda Firewall Control Center. The Control Center can be deployed either in the AWS or Azure public cloud, or on-premises.



Deploy via the Web Portal

The Barracuda CloudGen Firewall secures and connects the services running in your AWS virtual private cloud (VPC). The firewall monitors and secures all traffic between subnets to and from the Internet. It also connects your cloud resources either to your on-premises networks with site-to-site VPN, or to your remote users with client-to-site VPN and SSL VPN.

For more information, see How to Deploy a CloudGen Firewall in AWS via AWS Console.

Deploy via CloudFormation Template

CloudFormation templates are JSON files that include the definition of all your cloud resources. By launching the template via CloudFormation, you can automate your AWS deployments and create consistent environments for multiple purposes such as a deployment for production, cold standby, testing developing, etc.

For more information, see How to Deploy a CloudGen Firewall in AWS via CloudFormation Template.

Deploy Two CloudGen Firewalls in a High Availability Cluster in AWS

To avoid downtime when the primary firewall is unavailable due to maintenance or hardware failure, configure a high availability cluster. Incoming traffic is directed to the active firewall via Route 53 or the TCP-only AWS load balancer. The firewall then applies your policies and forwards the traffic accordingly to the backend. The AWS route table is monitored by the firewall. Routes where the destination is set to the firewall are updated by the active firewall after a failover event to ensure that the active firewall is always used as the gateway.

For more information, see High Availability in AWS.

Figures